Texte extrait de « CYBERDROIT 2009/2010, le droit à l'épreuve de l'internet »
5e édition, DALLOZ
Auteur: Christiane Féral-Schuhl

3. La cybersurveillance dans l'entreprise

Publié avec le soutien financier de la Commission Européenne

SECTION 0
ORIENTEUR

3.00

Plan du titre.

3.01

Textes applicables.

> Textes français.

C. trav., not. art. L. 1121-1, L. 1221-6, L. 2323-13, L. 2323-32 — C. pén., not. art. 226-15, 226-24 et 432-9 — L. n° 78-17, 6 janv. 1978, relative à l'informatique et aux libertés — L. n° 2004-801, 6 août 2004, relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978.

3.03

Bibliographie indicative.

> Rapports et Guide.

FDI, *Relations du travail et internet,* rapp. : panorama législatif et jurisprudentiel, 26 janv. 2006 — Cnil, H. Bouchet (dir.), *La cybersurveillance sur les lieux de travail,* mars 2004 — Cnil, *Guide pratique pour les employeurs.*

> Ouvrages.

M.-P. Fenoll-Trousseau et G. Haas, *La cybersurveillance dans l'entreprise et le droit : Traquer, être traqué,* Litec, 2002 — J.-E. Ray, *L'employeur, le salarié et les TIC,* Éd. Liaisons, 2007 ; *Le droit du travail à l'épreuve des NTIC,* Éd. Liaisons, Rueil-Malmaison, 2001 ; *Droit du travail – Droit vivant,* 15e éd., Éd. Liaisons, août 2006.

> Colloque.

Mardi de l'ADIJ (C. Baudoin), « Droit du travail et nouvelles technologies : actualités législatives et jurisprudentielles », compte-rendu J.-B. Auroux, *RLDI* n° 14, mars 2006, p. 83 ; compte-rendu L. Teyssandier, *Lexbase* N5659AKS

> Articles.

Numéro spécial de la revue *Dr. social,* « Le droit du travail à l'épreuve des NTIC », janv. 2002.

CHAPITRE

31. Contrôle de l'employeur sur l'outil de travail

SECTION 0
ORIENTEUR

31.00

Plan du chapitre.

Sect. 1 Pouvoirs de contrôle de l'employeur

Sect. 2 Devoirs de loyauté de l'employé

Sect. 3 Responsabilités

31.01

Textes applicables.

> Textes français.

V. s^s n^o 3.01.

L. n^o 2004-575, 21 juin 2004, pour la confiance dans l'économie numérique — L. n^o 82-689, 4 août 1982, relative aux libertés des travailleurs dans l'entreprise, *JO* 6 août, 2518.

31.02

Jurisprudence de référence.

> À propos de l'obligation générale de loyauté de l'employé.

• **Soc. 16 juin 1998,** *D.* 1998, IR 77.

* V. s^s n^o 31.21.

> Sur la mise en place de mots de passe sur les postes de travail.

• **Soc. 6 févr. 2001,** n^o 98-46.345, Sté Laboratoires pharmaceutiques Dentoria c/Mme Bardagiet et a., *Bull. civ.* V, n^o 43 ; *JCP G* 25 juill. 2001, n^o 30, p. 1514, note C. Puigelier ; *RTD civ.* oct.-déc. 2001, n^o 4, 880-882, note J. Mestre et B. Fages — cassation de **CA Toulouse, 4^e ch. soc., 23 oct. 1998.**

• **Soc. 18 oct. 2006,** n^o 04-48.025, Jérémy L… c/Sté Techni-Soft, *Bull. civ.,* n^o 308 ; *CCE* janv. 2007, note E. Caprioli, p. 40 s. — confirmation de **CA Rennes, ch. soc., 21 oct. 2004.**

* V. s^s n^o 31.24, égalt n^os 33.22 et 35.21.

> À propos de l'utilisation abusive des outils de l'entreprise.

• **Soc. 10 oct. 2007,** n^o 06-03.007, Claude G… c/Assoc. Ogec Emmanuel d'Alzon — confirmation de **CA Montpellier, ch. soc., 17 mai 2006,** Claude G… c/Assoc. Ogec Emmanuel d'Alzon, http://www.legalis.net/jurisprudence-decision.php3?id_article=2066 (consultation de sites pornographiques).

• Pour le jugement (confirmé) rendu en 1^er ressort, v. **Cons. prud'h. Montpellier, 26 sept. 2005,** Claude G… c/Assoc. Ogec Emmanuel d'Alzon.

* V. s^s n^o 31.23, égalt n^o 32.24.

• **Soc. 14 mars 2000,** n^o 1270, n^o 98-42.090, M. Dujardin c/Sté Instinet France *Bull. civ.* V, n^o 101 ; *Gaz. Pal.* 28 oct. 2000, n^o 302, p. 34, note J. Berenguer-Guillon et L. Guignot ; *JCP G* 7 févr. 2001, n^o 6, p. 325, note C. Puigelier ; *LPA* 11 juill. 2000, n^o 137, p. 5, note G. Picca et A. Sauret — confirmation par **CA Paris, 18^e ch., sect. A, 16 févr. 1998,** n^o 020563.

• Pour le jugement (infirmé partiellement) rendu en 1^er ressort, v. **Cons. prud'h. Paris, 2^e ch., sect. Encadrement, 13 déc. 1995.**

* V. s^s n^o 31.22, égalt n^os 32.11 et 30.23.

• **Soc. 11 mars 1998,** n^o 96-40.147, NPB, *RJS* 4/1998, n^o 415 — confirmation de **CA Paris, 21^e ch., sect. C, 7 nov. 1995.**

* V. s^s n^o 31.12, égalt. n^o 32.24 (utilisation abusive du téléphone).

• **CA Aix-en-Provence, 1^re ch. A, 25 nov. 2003,** n^o 2003/798.

* V. s^s n^o 31.21.

> À propos de la responsabilité de l'employeur.

• **Ass. plén. 19 mai 1988,** n^o 87-82.654, Cie d'assurance « La Cité », *Bull. civ.,* n^o 5 ; *RTD civ.* 1989, 89, obs. P. Jourdain

— confirmation de **CA Lyon, 24 mars 1987.**

* V. s^s n^o 31.32.

• Civ. 2^e, 19 juin 2003, n^o 00-22.626, AGV Vie et a. c/ Cts X… et a., *Bull. civ*. II, n^o 202 ; *D.* 2003, 1808 — cassation de **CA Lyon, 6^e ch. civ., 18 oct. 2000.**

* V. s^s n^o 31.23.

• CA Aix-en-Provence, 2^e ch., 13 mars 2006, SA Lucent Technologies c/ SA Lycos France, M. Nicolas B… — confirmation de **TGI Marseille, 11 juin 2003,** RG n^o 01/390.

* V. s^s n^o 31.33.

31.03

Bibliographie indicative.

> Rapports et Guide.

FDI, *Relations du travail et internet,* rapp., 17 sept. 2002 — Cnil, H. Bouchet (dir.), *La cybersurveillance sur les lieux de travail,* mars 2004 — Cnil, *Guide pratique pour les employeurs.*

> Articles.

J.-B. Auroux, « Les mardis de l'ADIJ : droit du travail et nouvelles technologies : actualités législative et jurisprudentielle », *RLDI* mars 2006 n^o 14, p. 83 ; v. aussi compte-rendu de L. Teyssandier, *Lexbase* N5659AKS — F. Bitan, « Messagerie électronique de l'entreprise : le pouvoir de contrôle de l'employeur à l'épreuve du secret des correspondances », *CCE* 2004, étude 15 — P. Bonneau, « Le contrôle des fichiers informatiques des salariés », *Décideurs : Stratégies, Finance & Droit* n^o 68, 15 août-15 sept. 2005, p. 52 s. — G. Haas et O. de Tissot, « Des restrictions inacceptables à la liberté d'action des syndicats », *Expertises* avr. 2005, p. 145 — D. Lebeau-Marianna, « Alertes éthiques : quelles orientations suite aux décisions de la Cnil ? », *RLDI* oct. 2005, n^o 9, p. 35 s. — M. Mélin et D. Melison, « Salarié, employeur et données informatiques : brefs regards croisés sur une pièce à succès », *RLDI* janv. 2007, n^o 23, p. 69 s. — A. Saint Martin, « Contrôle des messages électroniques du salarié et mesures d'instruction in futurum », *RLDI* juin 2007, n^o 28 ; « Une présomption de professionnalité des messages électroniques du salarié ? », *RLDI* mai 2007, n^o 27 — Étudiants du Master 2 de droit du multimédia et de l'informatique de l'Université de Paris II dirigé par le professeur J. Huet, « Le blog : nouvelle arme des salariés », *RLDI* n^o 27, mai 2007, p. 90 s.

31.04

Question principale.

• À quelles conditions l'employeur peut-il encadrer les conditions d'utilisation de l'accès internet au sein de son entreprise ?

* V. s^s n^o 31.12.

• Quelles sont les responsabilités de l'employé dans l'utilisation de l'internet sur son lieu de travail ?

* V. s^s n^o 31.21.

• L'employeur peut-il être responsable de la diffusion par un employé de contenus illicites ?

* V. s^s n^o 31.32.

31.09

L'accès internet est un outil de travail. L'accès internet, en particulier la messagerie, est devenu, à l'égal du téléphone, un outil de travail. Il s'avère en effet de plus en plus utile, voire indispensable dans l'exercice professionnel de la plupart des employés.

Or, l'employeur dispose sur cet outil d'un pouvoir de contrôle technique lui permettant d'intercepter les messages de son employé, de connaître les destinataires de ces messages, l'objet du message, la nature et le contenu des fichiers attachés, les sites consultés, les forums auxquels il participe… Il peut par exemple savoir si ses employés utilisent l'internet pour des motifs professionnels ou personnels, combien de temps ils passent à consulter l'internet, leurs horaires de consultation… Comme pour les autocommutateurs[1] téléphoniques, l'enregistrement automatique des adresses *e-mails* ou des sites *web* est susceptible de permettre de dresser un profil de l'employé et donc de collecter des informations sur sa vie privée (appartenances syndicales, politiques, intérêt pour la pornographie, le révisionnisme, *etc.*). Ces moyens permettent de « surveiller » les employés, de les « tracer » au travers des données émises ou reçues via l'internet, autant de pratiques dénoncées par la Commission nationale de

[1] V. aussi Cnil, *5^e Rapport d'activité,* p. 109 et *15^e Rapport d'activité,* p. 74, Doc. fr.

l'informatique et des libertés (Cnil), dès 2001, à l'occasion de son rapport[2] sur la « cybersurveillance » des employés par leurs employeurs.

Ceci pose inévitablement la question de la protection des libertés fondamentales de l'employé — c'est à ce titre que la Cnil a émis une série de recommandations sur la « cybersurveillance dans l'entreprise » — et celle, non moins difficile, des limites des droits de l'employé.

SECTION 1
POUVOIR DE CONTROLE DE L'EMPLOYEUR

31.11

Tolérance de l'usage à titre privé de l'outil de travail. L'accès à l'internet et la messagerie, un poste téléphonique sont autant de moyens mis à la disposition de l'employé pour lui permettre d'exécuter son travail. S'il existe une tolérance pour permettre leur utilisation à titre privé — à l'exemple du téléphone — tout est question de proportion. Que dire si, sur une centaine de *e-mails* échangés par jour, 75 % relevait de questions privées ? En effet, qu'il s'agisse de messages personnels échangés par *e-mails* ou de la consultation à titre personnel de sites internet, l'employeur subit la perte de temps de travail ainsi que les dépenses associées, notamment en heures de connexion. Un sondage aurait ainsi révélé que 20 à 50 % du temps passé sur l'internet en entreprise serait consacré aux loisirs.

31.12

Encadrement des conditions d'utilisation de l'outil de travail. Dans ce contexte, il apparaît légitime qu'un employeur s'assure du caractère non abusif de l'utilisation par ses employés des outils de travail mis à leur disposition. Il doit cependant agir en toute transparence et de manière « proportionnée »[3]. Il s'agit de rechercher, dans la ligne des principes énoncés par la Cnil et des préconisations du Forum des droits sur l'internet[4], le juste équilibre entre le pouvoir de contrôle de l'employeur et la protection des libertés fondamentales des employés.

La Cnil, dans son rapport « *La Cybersurveillance sur les lieux de travail »,* modifié le 18 décembre 2003, observait que si « une interdiction générale et absolue de toute utilisation d'internet à des fins autres que professionnelles, par les employés, ne paraît pas réaliste dans une société de l'information et de la communication, et semble, de plus, disproportionnée au regard des textes applicables », « un usage raisonnable, non susceptible d'amoindrir les conditions d'accès professionnel au réseau ne mettant pas en cause la productivité est généralement et socialement admis par la plupart des entreprises ou administrations ». Néanmoins, la Cnil estime que cet usage toléré de l'outil informatique et du réseau internet par un employé, à titre privé, peut être soumis à des conditions ou limites fixées par l'employeur. Ainsi, la Cnil préconise la mise en place de dispositifs de filtrage de sites non autorisés, associés au pare-feu, ainsi que la mise en œuvre d'un contrôle *a posteriori* des données de connexion à internet, restitué de façon globale (par exemple, au niveau de l'organisme ou d'un service de celui-ci), sans qu'il soit besoin de procéder à un contrôle individualisé des sites visités par un employé déterminé. En d'autres termes, l'employeur est fondé à encadrer les conditions d'accès à l'internet et d'utilisation de la messagerie à des fins personnelles. Il peut interdire l'accès à des sites à caractère illicite (contenu pornographique, pédophile, incitation au racisme, *etc.*) ou encore interdire le téléchargement de logiciels, la connexion à des forums ou à des *chats,* l'accès aux boîtes aux lettres personnelles à raison des risques de propagation de virus. Toutefois, lorsqu'un tel contrôle est réalisé par l'employeur, détaillé poste par

---

[2] H. Bouchet (dir.), *La cybersurveillance des employés dans l'entreprise,* Cnil, mars 2001, http://www.CNIL.fr/index.php?id=1432.

[3] Soc. 11 mars 1998, n° 1375, *RJS* 4/1998, n° 415.

[4] FDI, *Relations du travail et internet,* rapp. du FDI, 17 sept. 2002, http://www.foruminternet.org/recommandations/lire.phtml?id=394.

poste, ce dispositif doit faire l'objet d'une déclaration auprès de la Cnil.

SECTION 2
DEVOIR DE LOYAUTE DE L'EMPLOYE

31.21
Obligation générale de loyauté. Dans un premier temps favorable aux employés, les juges rappellent de plus en plus souvent que l'employeur est légitimement en droit d'attendre d'un employé qu'il exécute son contrat de travail dans le respect de l'obligation générale de loyauté[5].

Un arrêt de la cour d'appel d'Aix-en-Provence du 25 novembre 2003[6] souligne à ce titre que « l'ensemble des textes nationaux ou internationaux visant à protéger la vie privée notamment des salariés sur leur lieu de travail ne saurait créer une zone d'immunité ou d'impunité pour des fautes commises à l'encontre de son propre employeur ou de tiers ».

31.22
Jouer sur le lieu de travail. La Cour de cassation énonce, dans un arrêt en date du 14 mars 2000[7], que jouer sur le lieu de travail est « illégal »[8]. À ce titre, elle avait donné raison à l'employeur qui avait licencié pour faute grave son employé pour s'être livré, pendant son temps de travail et en utilisant le matériel de l'entreprise, à des jeux — notamment des paris sportifs — avec des tiers.

31.23
Consulter des sites pornographiques. De même, la consultation de sites pornographiques par un employé sur son lieu et pendant ses heures de travail est susceptible de conduire cet employé au licenciement, comme l'illustre un arrêt du 10 octobre 2007[9] de la chambre sociale de la Cour de cassation (rejet du pourvoi CA Montpellier, 17 mai 2006).

31.24
Mesures de sécurité. La Cnil rappelle que « l'ordinateur mis à la disposition du salarié peut être protégé par un mot de passe ou *log-in,* mais cette mesure de sécurité est destinée à éviter les utilisations malveillantes ou abusives par un tiers : elle n'a pas pour objet de transformer l'ordinateur de l'entreprise en un ordinateur à usage privé ». À ce titre, l'employé, seul détenteur du mot de passe, est tenu, lorsque l'employeur en fait la demande, de restituer les éléments matériels et de communiquer les informations qu'il détient et qui sont nécessaires à la poursuite de l'activité de l'entreprise[10].

De même, s'agissant de l'utilisation de moyens de cryptologie, la Cour de cassation a également considéré que l'employé qui chiffre volontairement l'accès à ses données, sur son poste informatique, sans l'autorisation de son employeur, commet une faute grave[11].

---

[5] Soc. 16 juin 1998, *D.* 1998, IR 77.
[6] CA Aix-en-Provence, 1re ch. A, 25 nov. 2003, no 2003/798.
[7] Soc. 14 mars 2000, no 98-42.090, *Bull. civ.* V, no 101 ; *Gaz. Pal.* 28 oct. 2000, no 302, p. 34, note J. Berenguer-Guillon et L. Guignot ; *JCP G* 7 févr. 2001, no 6, p. 325, note C. Puigelier ; *LPA* 11 juill. 2000, no 137, p. 5, note G. Picca et A. Sauret.
[8] F. Lemaître, « Jouer sur le lieu de travail est illégal, estiment les juges », *Le Monde* 28 mars 2000.
[9] Soc. 10 oct. 2007, no 06-43.816, rejet du pourvoi CA Montpellier, 17 mai 2006, v. http://www.legalis.net/jurisprudence-decision.php3?id_article=2065.
[10] Soc. 6 févr. 2001, no 98-46.345, *Bull. civ.* V, no 43 ; *JCP G* 25 juill. 2001, no 30, p. 1514, note C. Puigelier ; *RTD civ.* oct.-déc. 2001, no 4, p. 880-882, note J. Mestre et B. Fages.
[11] Soc. 18 oct. 2006, *CCE* janv. 2007, note E. Caprioli, p. 40 s.

SECTION 3
RESPONSABILITES

31.31

Responsabilité de l'employé dans l'exercice de sa liberté d'expression. Sur le terrain de la liberté d'expression, l'employé bénéficie d'un droit d'expression dans et hors de l'entreprise, comme le rappelle la loi du 4 août 1982 qui lui reconnaît « un droit à l'expression directe et collective sur le contenu, les conditions d'exercice et l'organisation de leur travail » (sur les principes généraux pour le respect de la vie privée de l'employé v. s^{s} n^{os} 34.00 s).

Cependant, la jurisprudence rappelle que ce principe a pour corollaire celui de la responsabilité de ceux qui en usent. S'il est exact que la subordination inhérente au contrat de travail n'a pas pour effet de priver l'employé des droits fondamentaux attachés à sa personne, et notamment de sa liberté d'opinion, de conscience et d'expression, il n'en reste pas moins que « l'exécution loyale du contrat lui impose une obligation de discrétion tant vis-à-vis des tiers que vis-à-vis des autres employés de l'entreprise »[12]. Aussi, l'employé qui exerce son droit d'expression doit-il le faire sans que cela ne conduise à des abus tels que le dénigrement des personnes et des dénonciations calomnieuses.

Cette dernière jurisprudence permet de circonscrire les conditions d'utilisation des « défouloirs électroniques »[13] qui se généralisent, soit dans le cadre de forums créés à cet effet par l'employeur, soit dans le cadre de sites ou forums créés à l'initiative d'un employé ou d'un groupe d'employés.

Par ailleurs, il convient de préciser que la règle de discrétion s'impose également aux représentants des salariés (sur les limites posées à la liberté de communication syndicale v. s^{s} n^{o} 37.14).

31.32

Responsabilité de l'employeur à raison de certaines dérives de salariés. L'article 1384 alinéa 5 du Code civil énonce un principe de responsabilité civile de l'employeur en cas de faute commise par l'un de ses employés ayant agi dans le cadre de ses fonctions. C'est ce que l'on appelle la responsabilité du commettant du fait de ses préposés.

Le rattachement de la faute de l'employé à ses fonctions est apprécié par la jurisprudence en fonction du lien de connexité entre la faute et l'exécution du contrat de travail. Cette connexité est généralement retenue lorsque la faute est commise par l'employé pendant le temps de travail, sur le lieu de travail, avec les moyens mis à sa disposition par l'employeur, par la mise en oeuvre des instructions de l'employeur ou encore avec la volonté d'agir pour le compte de l'employeur. La jurisprudence retient également la responsabilité de l'employeur pour des actes commis par l'un de ses employés en dehors du temps et du lieu de travail, avec des moyens personnels ou non, commandés par l'employeur lorsque les actes sont susceptibles d'être considérés comme rattachés aux fonctions. En effet, si une jurisprudence ancienne refusait de rendre l'employeur responsable du dommage causé avec un instrument de travail lorsqu'il avait été occasionné en dehors du lieu et du temps de travail, la solution est devenue moins tranchée désormais et de nombreux arrêts rattachent aux fonctions des dommages causés par le seul usage d'une chose ou d'un outil de travail, comme par exemple un blog, ou un forum.

L'employeur n'est évidemment pas responsable lorsque la faute de l'employé ne peut être rattachée à ses fonctions et est sans rapport avec celles-ci. Si la faute est susceptible d'être rattachée aux fonctions, l'employeur peut s'exonérer de sa responsabilité s'il démontre trois conditions cumulatives définies par la Cour de cassation[14] : l'employé a agi en dehors de ses fonctions, sans autorisation et à des fins étrangères à ses attributions. C'est sur la base des trois conditions précitées qu'un arrêt de la cour d'appel d'Aix-en-Provence a sanctionné un employeur à

---

[12] *Francis Lefebvre,* PB II, feuillet 1.

[13] M.-J. Gros et L. Lamprière, « J'irai cracher sur ma boîte », archives payantes du journal Libération.

[14] Ass. plén. 19 mai 1988, n^{o} 87-82.654, *RTD civ.* 1989, 89, obs. P. Jourdain.

raison de l'utilisation fautive d'internet par un de ses salariés. Dans le cas d'espèce, l'employé avait pris l'initiative de diffuser une page personnelle sur le web critiquant une société tierce. Les juges ont rappelé à cette occasion qu'il revient à l'employeur de « contrôler le bon usage par les salariés d'un outil appartenant à l'entreprise ». Ils ont considéré que l'employé (i) avait agi dans le cadre de ses fonctions car il avait trouvé dans ses fonctions l'occasion et les moyens, notamment informatiques, de commettre un acte illicite, (ii) avait agi avec l'autorisation de l'employeur qui avait, dans une note interne, déclaré tolérer l'usage personnel et licite de l'internet, (iii) n'avait pas agi à des fins étrangères à ses attributions au motif que le règlement intérieur l'autorisait à disposer d'un accès à l'internet en dehors même de ses horaires de travail[15].

Une décision tout aussi sévère a été prononcée par la Cour de cassation au sujet d'un agent d'assurances qui avait commis divers détournements avec des moyens informatiques pendant son temps de travail et sur son lieu de travail : « La préposée avait agi au temps et au lieu de travail à l'occasion des fonctions auxquelles elle était employée, avec le matériel mis à sa disposition, ce qui excluait qu'elle ait commis ses détournements en dehors de ses fonctions. »

Enfin, la cour d'appel de Paris a retenu la faute de l'employeur qui avait laissé ses employés se connecter sans contrôle à des sites (fichers multimédia, de jeux, pornographiques, *etc.*), sans lien avec leur activité professionnelle. Dans cette affaire, l'employeur était en litige avec son prestataire de sauvegarde de données informatiques et de protection antivirus. Alors que les juges de première instance avaient retenu que « la présence de virus dans l'installation (du client) est la preuve que [le fournisseur] n'a pas correctement exécuté l'action anti-virus », la cour d'appel a considéré que le client « en laissant son personnel se connecter à de tels sites, a rendu, par sa faute, inefficace la protection que [le fournisseur] s'était engagé à lui fournir de sorte qu'elle ne pouvait invoquer la défaillance de la protection anti-virus comme un juste motif de la résiliation des contrats »[16].

Cependant, il a pu être jugé que le seul fait de tenir un blog personnel en ligne ne suffit pas à justifier d'une atteinte à la réputation de son employeur (Cons. prud'h, 30 mars 2007, v. s^{s} n^{o} 125.28).

Ces jurisprudences démontrent l'utilité à définir, dans le règlement intérieur ou en annexe à celui-ci, les conditions dans lesquelles les employés peuvent utiliser les ressources informatiques et l'accès à l'internet mis à leur disposition professionnelle.

[15] TGI Marseille, 1re ch. civ., 11 juin 2003, Escota c/Lucent Technologies, http://www.juriscom.net ; confirmé par CA Aix-en-Provence, 13 mars 2006, pourvoi no 2006/170.

CHAPITRE

32. Principe de transparence

SECTION 0
ORIENTEUR

32.00

Plan du chapitre.

Sect. 1 Obligation d'information

Sect. 2 Conséquences en cas de défaut de transparence

32.01

Textes applicables.

> Textes français.

V. s^{s} n^{o} 3.01.

32.02

Jurisprudence de référence.

> Sur l'obligation d'information des employés.

• **Soc. 22 mai 1995,** n° 93-44.078, *Bull. civ.* V, n^{o} 164 ; *Rev. soc. Francis Lefebvre* 1995, n^{o} 7, p. 489, note Y. Chauvy — confirmation de **CA Douai, 30 juin 1993.**

* V. s^{s} n^{o} 32.11, égalt s^{s} n^{o} 30.23.

> Sur l'obligation d'information et de consultation du comité d'entreprise.

• **Soc. 7 juin 2006,** n^{o} 04-43.866, Girouard c/Continent France, *Bull. civ.* V, n^{o} 206 ; *D.* 2006, 1704 — confirmation de **CA Bourges ch. soc., 24 oct. 2003.**

* V. s^{s} n^{o} 32.12 et égalt n^{o} 30.24.

> Récusation des moyens de preuve pour défaut d'information des employés.

• **Soc. 6 juin 2007,** n^{o} 05-43.996, sté Eliophot c/M. X — confirmation de **CA Aix-en-Provence, 18^{e} ch., 7 juin 2005.**

• **Soc. 2, 20 nov. 1991,** n^{o} 88-43.120, *Bull. civ.* V, n^{o} 519 ; *D.* 13 févr. 1992, n^{o} 7, 73, note Y. Chauvy — cassation de **CA Colmar, ch. soc., 17 déc. 1987.**

* V. s^{s} n^{o} 32.11 et 32.22, égalt n^{o} 30.23.

• **CA Paris, 31 mai 1995,** *Juris-Data* n^{o} 024755 ; *RLDI* mai 2007, n^{o} 27, comm. A. Saint Martin.

* V. s^{s} n^{o} 32.23.

> Récusation des moyens de preuve pour manquement aux règles Cnil.

• **CA Paris, 7 mars 1997,** *Gaz. Pal.* 21 janv. 1999.

V. égalt **CA Paris, 31 mai 1995** (préc.).

* V. s^{s} n^{o} 32.23.

>Admission à titre de preuve des relevés d'appels téléphoniques.

• **Soc. 29 janv. 2008,** n^{o} 06-45.279, Touati c/sté Canon France, *JS Lamy* 2008, n^{o} 228, comm. J.-E. Tourreil ; *Gaz. Pal.* 24 avr. 2008, n^{o} 115, p. 39, note L. Boncourt — confirmation de **CA Versailles, 11^{e} ch., 5 sept. 2006.**

* V. s^{s} n^{o} 32.23.

>Admission de la preuve.

• **Soc. 11 mars 1998,** n^{o} 96-40.147, Pisani c/sté Pisani, *Sem. soc. Lamy* 28 mai 2001, n^{o} 1030 — confirmation de **CA Paris, 21^{e} ch., 7 nov. 1995.**

* V. s^{s} n^{o} 32.24.

• **CA Montpellier, 17 mai 2006,** n^{o} 05/01954, Claude G… c/Assoc. Ogec Emmanuel d'Alzon, http://www.legalis.net/jurisprudence-decision.php3?id_article=2066 — confirmation par **Soc. 10 oct. 2007,** n^{o} 06-03.007, Claude G… c/Assoc. Ogec Emmanuel d'Alzon.

• Pour le jugement (confirmé) rendu en premier ressort, v. **Cons. prud'h. Montpellier, 26 sept. 2005,** Claude G… c/Assoc. Ogec Emmanuel d'Alzon.

* V. s^{s} n^{o} 32.24, égalt n^{o} 31.23.

• V aussi **Soc. 10 oct. 2007,** Claude G… c/Assoc. Ogec Emmanuel d'Alzon (préc.)

* V. s^{s} n^{o} 32.24.

• **CA Aix-en-Provence, 18^{e} ch., 4 janv. 1994**, Perez c/Beli Intermarchés, *Dr. soc.* 1995, 332 ; S. Darmaisin, « L'ordinateur, l'employeur et le salarié », *Dr. soc.* 2000, p. 580 ; *Juris-Data* n^{o} 041281 — infirmation de **Cons; pud'h. Nice, sect. comm., 10 déc. 1990**.

* V. s^s n^o 32.25.

• **Soc. 14 mars 2000,** n^o 1270, n° 98-42.090, *Bull. civ.* V, n^o 101 ; *Gaz. Pal.* 28 oct. 2000, n^o 302, p. 34, note J. Berenguer-Guillon et L. Guignot ; *JCP G* 7 févr. 2001, n^o 6, p. 325, note C. Puigelier — confirmation par **CA Paris, 18^e ch., sect. A, 16 févr. 1998,** n^o 020563.

Pour le jugement (infirmé partiellement) rendu en premier ressort, v. **Cons. prud'h. Paris, 2^e ch., sect. Encadrement, 13 déc. 1995**.

* V. s^s n^os 32.11 et 32.24, égalt. s^s n^os 30.23 et 31.22.

> Sur la valeur juridique des chartes.

• **Soc. 21 déc. 2006,** n^o 05-41.165, J.-H. Pettre c/sté Ad 2 One SA — confirmation de **CA Versailles, 5^e ch., sect. B, 25 nov. 2004.**

* V. s^s n^o 32.15.

> Sur l'admission des moyens de preuve en matière pénale.

• **Crim. 6 avr. 1994,** n^o 93-82.717, *Bull. crim.,* n^o 136 — confirmation de **CA Bordeaux, 3^e ch., 13 mai 1993.**

• **Crim. 23 juill. 1992,** n^o 92-82.721, *Bull. crim.,* n^o 274 — confirmation de **CA Caen, ch. acc., 8 avr. 1992.**

• **Crim. 31 mai 2005,** n^o 04-85.469 — confirmation de **CA Montpellier, ch. corr., 6 mai 2004.**

* V. s^s n^o 32.26, égalt n^os 30.26 et 30.23.

32.04

Questions principales.

• Quelles sont les conditions de la licéité de la collecte et du traitement des données à caractère personnel ?

* V. s^s n^os 32.11 et 32.12.

• Quelles sont les conséquences juridiques en cas de non respect des obligations d'information des employés ?

* V. s^s n^o 32.22.

SECTION 1
OBLIGATION D'INFORMATION

32.11

Obligation d'information des employés. Le Code du travail prévoit expressément qu'« aucune information concernant personnellement un employé (ou un candidat à un emploi) ne peut être collectée par un dispositif qui n'a pas été porté préalablement à la connaissance de l'employé (ou du candidat à un emploi) » (C. trav., art. L. 1221-9 [anc^t art. L. 121-8]). La Commission nationale de l'informatique et des libertés (Cnil) rappelle également que les employés concernés doivent toujours être individuellement informés de la mise en œuvre des dispositifs de contrôle, des modalités de leur droit d'accès aux données et de la finalité des mesures de contrôle.

Cette règle a été rappelée par la Cour de cassation à plusieurs reprises : « Si l'employeur a le droit de contrôler et de surveiller l'activité de son personnel durant le temps de travail, il ne peut mettre en œuvre un dispositif de contrôle qui n'a pas été porté préalablement à la connaissance des salariés.[17] » Ou encore : « L'employeur a le droit de contrôler et de surveiller l'activité de ses salariés pendant le temps de travail, l'emploi de procédé clandestin de surveillance étant toutefois exclu[18] ».

On constate ainsi que ce n'est pas tant la mise en place de dispositifs pour contrôler et surveiller les employés que le fait d'y procéder à leur insu qui est condamnable. Il est donc prudent d'organiser, dans le cadre d'un règlement intérieur ou d'un code de conduite ou encore d'une « charte », les conditions d'utilisation des accès internet, notamment de la messagerie, et d'y faire référence dans les contrats de travail. Ces conditions d'utilisation peuvent par ailleurs être rappelées au moment de l'attribution d'un code d'accès ou sur certaines pages écran ou encore dans la diffusion de notes de service. La Cnil « en soutient

[17] Soc. 20 nov. 1991, n^o 88-43.120, *Bull. civ.* V, n^o 519 ; *D.* 13 févr. 1992, n^o 7, 73, note Y. Chauvy : s'agissant d'une caméra dissimulée — Soc. 22 mai 1995, n^o 93-44.078, *Bull. civ.* V, n^o 164 ; *Rev. soc. Francis Lefebvre* 1995, n^o 7, p. 489, note Y. Chauvy : s'agissant de la filature d'un salarié par un détective privé.

[18] Soc. 14 mars 2000, n^o 1270, n^o 98-42.090, *Bull. civ.* V, n^o 101 : à propos d'un système d'écoute des conversations téléphoniques.

l'initiative lorsque ces « chartes » ou « guides des bons usages » se fixent pour objectif d'assurer une parfaite information des utilisateurs, de sensibiliser les employés ou les agents publics aux exigences de sécurité, d'appeler leur attention sur certains comportements de nature à porter atteinte à l'intérêt collectif de l'entreprise ou de l'administration »[19].

32.12

Obligation d'information et de consultation du comité d'entreprise. Lorsqu'il existe un comité d'entreprise, l''employeur a également l'obligation de l'informer avant de mettre en œuvre des « traitements automatisés de la gestion du personnel et sur toute modification de ceux-ci » (C. trav., art. L. 2323-32 ; anc. L. 432-2-1)[20]. Il doit également le consulter préalablement à tout projet important d'introduction de « nouvelles technologies, lorsque celles-ci sont susceptibles d'avoir des conséquences sur l'emploi, la qualification, la rémunération, la formation ou les conditions de travail du personnel » (C. trav., art. L. 2323-13 ; anc. L. 432-2, al. 1). Enfin, il doit l'informer et le consulter « préalablement à la décision de mise en œuvre dans l'entreprise, sur les moyens ou les techniques permettant un contrôle de l'activité des employés » (C. trav., art. L. 2323-32). L'information à fournir au comité d'entreprise doit être précise et écrite (C. trav., art. L. 2323-4 ; anc. L. 431-5, al. 2). Cependant, l'avis exprimé par le comité d'entreprise est purement consultatif et ne lie pas l'employeur.

La connexion à l'internet, la création d'un réseau intranet, la mise en place d'une messagerie électronique constituent à l'évidence « une nouvelle technologie et une technique permettant un contrôle de l'activité des employés » au sens de ce qui précède. Plus généralement, on retiendra que l'employeur doit informer et consulter le comité d'entreprise (C. trav., art. L. 1221-9 ; anc. L.121-8) ou, dans la fonction publique, le comité technique paritaire ou toute instance équivalente, préalablement à la mise en œuvre d'un système de traitements ou de procédures permettant de « tracer » les employés dans leurs activités, par exemple permettant d'accéder au poste d'un employé absent.

Le dossier de déclaration auprès de la Cnil doit d'ailleurs comporter l'indication et la date à laquelle les instances représentatives du personnel ont été consultées..

La Cour de cassation a eu l'occasion de sanctionner l'absence de consultation du comité d'entreprise en application de l'article L. 432-2-1 (devenu art. L. 2323-32) du Code du travail, quand bien même il ne pouvait être sérieusement contesté que les salariés ignoraient la présence de caméras puisque celles-ci étaient utilisées depuis longtemps et des affichettes mentionnaient leur présence[21].

32.13

Chartes « internet » et Code du travail. L'employeur peut soumettre à la signature de ses employés un document fixant les conditions d'usage des outils informatiques dans l'entreprise. Un tel document peut être annexé au contrat de travail.

Si ce texte prévoit des injonctions de faire, des interdictions, ou des sanctions disciplinaires, il constitue une adjonction au règlement intérieur. Dans cette hypothèse, ce texte fait l'objet de conditions de publication et d'information plus lourdes : il doit, en effet, faire l'objet d'une information et d'une consultation du comité d'entreprise, d'une communication à l'inspection du travail, d'un dépôt auprès du conseil de prud'hommes et d'un affichage. Ce document permet d'établir les règles internes de déontologie et de sécurité relatives à l'utilisation de l'informatique et des réseaux. La rédaction d'un tel code de conduite comporte plusieurs avantages : s'il permet de prévenir l'employeur d'éventuels litiges l'opposant à ses employés, il remplit également l'obligation d'information quant aux systèmes de contrôle des employés mis en place dans l'entreprise, tant à

---

[19] H. Bouchet (dir.), *La cybersurveillance sur les lieux de travail,* rapp. Cnil, mars 2004, http://www.CNIL.fr/index.php?id=1432.

[20] Pour la fonction publique, l'employeur est tenu de consulter le comité technique ou tout autre organisme équivalent du comité d'entreprise : v. L. n° 84-16, 11 janv. 1984 ; L. n° 84-53, 26 janv. 1984 et L. n° 86-33, 9 janv. 1986.

[21] Soc. 7 juin 2006, n° 04-43.866, Girouard c/Continent France, *Bull. civ.* V, n° 206 ; *D.* 2006, 1704.

l'égard des employés, qu'à l'égard des instances représentatives du personnel.

32.14
Chartes « internet » et Cnil. Selon la Cnil, le document adopté « doit préciser les potentialités techniques des outils et les utilisations effectivement mises en œuvre, notamment en matière d'utilisation des traces ». Plus précisément, doivent être mentionnées dans cette charte, les modalités du contrôle mis en place, les systèmes de sauvegarde utilisés par l'employeur, ainsi que la durée des sauvegardes.

Dans son rapport d'étude et de consultation publique sur *La cybersurveillance des employés dans l'entreprise,* publié en mars 2001, ainsi que dans son rapport, intitulé *La cybersurveillance sur les lieux de travail,* modifié le 18 décembre 2003, la Commission nationale de l'informatique et des libertés (Cnil) met en garde contre les dérives et les abus qui ont souvent été rencontrés lors de la rédaction de chartes d'utilisation du matériel informatique. Le déséquilibre entre l'employeur et ses employés, au moment de la signature d'un tel document s'avère, selon la commission, souvent manifeste. Elle soutient néanmoins l'initiative de la création de telles chartes lorsque celles-ci se fixent pour objectif « d'assurer une parfaite information des utilisateurs, de sensibiliser [les employés] aux exigences de sécurité, d'appeler leur attention sur certains comportements de nature à porter atteinte à l'intérêt collectif de l'entreprise ».

32.15
« Chartes » et statut juridique. Un arrêt, rendu par la chambre sociale de la Cour de cassation, reconnaît aux chartes informatiques une valeur juridique et les place, aux côtés du règlement intérieur, comme documents opposables aux employés. Dans le cas d'espèce, le comportement d'un salarié qui avait tenté, sans motif légitime et par emprunt du mot de passe d'un autre salarié, de se connecter sur le poste informatique du directeur de la société, a été jugé contraire à l'obligation de respect de la charte informatique en vigueur dans l'entreprise. Un tel comportement constituait une faute grave et rendait impossible son maintien dans l'entreprise pendant la durée du préavis[22].

SECTION 2
CONSEQUENCES EN CAS DE DEFAUT DE TRANSPARENCE

32.21
Atteinte à la vie privée. Le Code du travail précise que la collecte et le traitement de données personnelles à l'insu des employés peuvent engager la responsabilité de l'employeur pour manquement à son obligation générale de transparence. Aussi, à défaut d'avoir informé le comité d'entreprise (ou dans la fonction publique, le comité technique paritaire ou toute instance équivalente) et les employés dans les conditions indiquées précédemment, un système de contrôle de la messagerie de l'employé ou encore un dispositif de traçage pour identifier les sites *web* qu'il a consultés pourrait être considéré comme portant atteinte à la vie privée de celui-ci. De même l'installation d'un dispositif installé à l'insu des employés de façon délibérément non visible (des caméras par exemple) ou visant à surveiller les allées et venues des employés sera considérée comme portant atteinte à la vie privée des employés.

La jurisprudence a dessiné les contours juridiques de la mise en œuvre de dispositifs de surveillance des employés, notamment en se fondant sur l'admission ou la récusation de moyens de preuve, fondés sur des systèmes de cybersurveillance.

32.22
Récusation des moyens de preuve pour défaut d'information des employés. L'employeur ne peut pas recourir à des moyens de preuve obtenus à l'aide de

[22] Soc. 21 déc. 2006 n° 05-41.165, NPB, J.-H. Pettre c/sté Ad 2 One SA : rejet du pourvoi contre CA Versailles, 5e ch. B, 25 nov. 2004 ; *Gaz. Pal.*, 07 août 2007, n° 219, p. 22.

procédés de contrôle qui n'auraient pas été portés préalablement à la connaissance des employés. De telles preuves seraient rejetées des débats judiciaires et les sanctions éventuelles prises à l'encontre des employés, sur la base de ces preuves, pourraient être annulées.

La Cour de cassation a précisé dès 1991, que « si l'employeur a le droit de contrôler et de surveiller l'activité de ses salariés pendant le temps de travail, tout enregistrement, quels qu'en soient les motifs, d'images ou de paroles à leur insu, constitue un mode de preuve illicite »[23]. Il s'agissait, dans le cas d'espèce, du licenciement d'une employée d'un magasin pour faute grave fondé sur un enregistrement produit au moyen d'une caméra dissimulée dans la caisse de l'intéressée.

Plus récemment, un arrêt de la Cour de cassation, en date du 6 juin 2007 a approuvé un arrêt de la cour d'appel qui, relevant le caractère privé du courrier électronique adressé par l'employé à l'un des ses collègues de travail, en a déduit que cet élément de la vie personnelle de l'intéressé ne pouvait constituer un motif de licenciement[24].

32.23

Récusation des moyens de preuve pour manquement aux règles Cnil. Les juges ont récusé la preuve rapportée par un traitement d'informations nominatives, régulièrement déclaré à la Cnil, considérant que l'information en cause est sans rapport avec la finalité du traitement[25]. Ainsi, à titre d'exemple, ne pouvait pas être utilisé, à l'insu du personnel, pour contrôler le temps de travail de celui-ci, un système informatique de réservation de billet, mis à la disposition des employés.

De même, l'arrêt du 7 mars 1997 de la cour d'appel de Paris a pu juger que la production en justice d'un listing de relevés de communications téléphoniques émanant du poste d'un salarié et obtenu au moyen d'un autocommutateur était illicite au motif qu'« en toute hypothèse, l'obligation de déclaration préalable faite à l'entreprise par l'article 6 de la loi du 6 janvier 1978 n'avait pas été respectée, et que ce relevé ne pouvait être conservé pour un motif autre que la facturation éventuelle à la salariée de ses communications personnelles »[26].

Cependant, il convient de signaler cet arrêt de la Cour de cassation en date du 29 janvier 2008 qui a admis que les relevés d'appels téléphoniques produits par l'employeur pouvaient justifier le licenciement de l'employé pour utilisation abusive de son téléphone professionnel[27]. Ces relevés établissaient que l'employé avait téléphoné, depuis son poste de travail, à des messageries de rencontre entre adultes, totalisant 63 heures entre juillet 2002 et janvier 2003. Le salarié a vainement tenté de se prévaloir de l'irrecevabilité de la preuve produite, arguant qu'il n'avait pas été informé du procédé de contrôle. Mais la Haute juridiction a considéré que la simple vérification des relevés de la durée, du coût et des numéros des appels téléphoniques passés à partir de chaque poste, édités au moyen de l'autocommutateur téléphonique de l'entreprise, ne constitue pas un procédé de surveillance illicite pour ne pas avoir été préalablement porté à la connaissance du salarié. On notera cependant que la question de la conformité à la loi informatique et libertés de la collecte de données personnelles des employés au travers des relevés téléphoniques n'a pas été soulevée en l'espèce.

32.24

Admission des moyens de preuve. Les juges ont considéré que l'employeur pouvait se prévaloir de l'enregistrement des conversations téléphoniques de son employé établissant que celui-ci s'était livré pendant le temps du travail à des jeux de hasard

---

[23] Soc. 20 nov. 1991, n° 88-43.120, *Bull. civ.* V, n° 519.

[24] Soc. 6 juin 2007, n° 05-43.996, NPB, sté Eliophot c/M. X… : rejet du pourvoi contre CA Aix-en-Provence, 18e ch., 7 juin 2005.

[25] CA Paris, 31 mai 1995, *Juris-Data* n° 024755 ; *RLDI* mai 2007, n° 27, comm. A. Saint Martin.

[26] CA Paris, 7 mars 1997, *Gaz. Pal.* 21 janv. 1999, p. 30.

[27] Soc. 29 janv. 2008, n° 06-45.279, Touati c/sté Canon France, *JS Lamy* 2008, n° 228, comm. J.-E. Tourreil ; *Gaz. Pal.* 24 avr. 2008, n° 115, p. 39, note L. Boncourt ; http://www.legifrance.gouv.fr/affichJuriJudi.do?oldAction=rechJuriJudi&idTexte=JURITEXT000018074945.

avec des tiers (paris sur l'élection présidentielle, résultats de matchs de football) car celui-ci avait été prévenu qu'il était enregistré[28]. Ils ont confirmé que « l'employeur a le droit de contrôler et surveiller l'activité de ses salariés pendant le temps du travail ; que seul l'emploi de procédé clandestin de surveillance est illicite »[29]. Dans le cas d'espèce, on notera qu'il s'agissait d'une société de bourse dont la réglementation professionnelle autorise l'enregistrement des ordres d'achat passés par téléphone.

De même, un arrêt du 11 mars 1998 prononcé par la chambre sociale de la Cour de cassation a admis que « ne constitue pas un mode de preuve illicite la production par l'employeur des relevés de facturation téléphonique qui lui ont été adressés par la société France Télécom pour le règlement des communications correspondant au poste du salarié »[30]. Ou encore, plus récemment, un arrêt de la cour d'appel de Montpellier du 17 mai 2006 a admis que les faits révélés à l'occasion de l'intervention de l'entreprise gestionnaire du système informatique de l'établissement appelée par le salarié qui se plaignait de la présence d'un virus informatique sur son poste de travail, avaient été licitement portés à la connaissance de l'employeur[31]. Les juges ont estimé que le licenciement pour faute grave était justifié, considérant que le salarié, en consultant à plusieurs reprises des sites pornographiques, avait failli à ses obligations d'enseignant et d'éducateur « de conserver la dignité inhérente à sa fonction et de respecter le caractère propre de l'établissement », figurant à la convention collective des professeurs du secondaire de l'enseignement privé. La chambre sociale de la Cour de cassation, dans un arrêt du 10 octobre 2007, a confirmé cette analyse[32].

32.25

En tout état de cause, les juges exigent des preuves de bonne qualité. Ainsi, un arrêt du 4 janvier 1994 de la cour d'appel d'Aix-en-Provence a précisé que le document de preuve produit doit présenter « des garanties suffisantes d'authenticité, d'impartialité et de sincérité concernant tant sa date que son contenu »[33].

(Pour des développements plus complets sur la difficulté d'établir la preuve v. s^s n^os 141.31.)

32.26

En matière pénale. La Cour de cassation a également rappelé qu'« aucune disposition légale ne permet aux juges répressifs d'écarter les moyens de preuve produits par les parties au seul motif qu'ils auraient été obtenus de façon illicite ou déloyale […] il leur appartient seulement […] d'en apprécier la valeur probante »[34]. Ou encore qu'« aucun texte de procédure pénale n'interdit la production par le plaignant à l'appui de sa plainte, de pièces de nature à constituer des charges contre les personnes visées dans celle-ci […] il appartient aux juridictions pénales d'en apprécier la valeur au regard des règles relatives à l'administration de la preuve des infractions »[35].

Ainsi, et à titre d'exemples, on peut citer le cas de l'enregistrement de l'activité d'une officine pharmaceutique par une caméra installée dans un endroit ouvert au public à la diligence du pharmacien qui a permis de démontrer l'abus de confiance commis à son préjudice par un employé. Ou encore le cas d'un employé poursuivi

---

[28] F. Lemaître, dans « Jouer sur le lieu de travail est illégal, estiment les juges », *Le Monde* 28 mars 2000.

[29] Soc. 14 mars 2000, n° 1270, n° 98-42.090, *Bull. civ.* V, n° 101 ; *Gaz. Pal.* 28 oct. 2000, n° 302, p. 34, note J. Berenguer-Guillon et L. Guignot ; *JCP G* 2001, n° 6, p. 325, note C. Puigelier.

[30] Soc. 11 mars 1998, n° 96-40147 Pisani c/sté Pisani, *Sem. soc. Lamy* 28 mai 2001, n° 1030, v. http://www.legifrance.gouv.fr/affichJuriJudi.do?oldAction=rechExpJuriJudi&idTexte=JURITEXT000007373394.

[31] CA Montpellier, 17 mai 2006, n° 05/01954, Claude G… c/Assoc. Ogec Emmanuel d'Alzon, v. http://www.legalis.net/jurisprudence-decision.php3?id_article=2066

[32] Soc. 10 oct. 2007, n° 06-03.007 ; rejet du pourvoi CA Montpellier, 17 mai 2006, v. http://www.legalis.net/jurisprudence-decision.php3?id_article=2065.

[33] CA Aix-en-Provence, 4 janv. 1994, *Dr. soc.* 1995, 332. ; S. Darmaisin, « L'ordinateur, l'employeur et le salarié », *Dr. soc.* 2000, p. 580.

[34] Crim. 6 avr. 1994, n° 93-82.717, *Bull. crim.,* n° 136.

[35] Crim. 23 juill. 1992, n° 92-82.721, *Bull. crim.,* n° 274.

pour vol en réunion sur la base d'un enregistrement du système de vidéosurveillance montrant deux personnes emportant divers objets en les faisant passer par la fenêtre du local des toilettes et en les déposant dans un véhicule placé à proximité de cette fenêtre[36].

Cependant, on notera que la Cour de cassation a confirmé à au moins deux reprises, qu'il n'est pas possible de recourir à la provocation policière pour établir la preuve d'infractions (Crim. 7 févr. 2007[37] — Crim. 4 juin 2008[38] — développements v. s^{s} n^{o} 143.12).

[36] Crim. 31 mai 2005, n^{o} 04-85.469.

[37] Crim. 7 févr. 2007, n^{o} 06-87.753, *Bull. crim.,* n^{o} 37 ; cass. CA Paris, 26 sept. 2006 (renvoi devant CA Versailles) ; v. également « Une procédure fondée sur une provocation à commettre une infraction, même commise à l'étranger, doit être annulée », *AJ pénal* 2007, n^{o} 5, mai, juri. p. 233.

[38] Crim. 4 juin 2008, n^{o} 08-81.045 ; , P ; *JCP G* 2008, IV, 2287 ; http://www.legifrance.gouv.fr/affichJuriJudi.do?oldAction=rechJuriJudi&idTexte=JURITEXT000018946415.

CHAPITRE

33. Principe de proportionnalité

SECTION 0
ORIENTEUR

33.00

Plan du chapitre.

33.01

Textes applicables.

> Textes français.

Textes législatifs.

V. s^s n^o 3.01.

Avis et recommandations.

Cnil, doc. d'orientation adopté par la Commission le 10 nov. 2005 pour la mise en œuvre de dispositifs d'alerte professionnelle conformes à la loi du 6 janvier 1978 (modifiée en août 2004) – Cnil, délib. n^o 2005-305, 8 déc. 2005, portant autorisation unique de traitements de données à caractère personnel mis en œuvre dans le cadre de dispositifs d'alerte professionnelle — Cnil, délib. n^o 2006-067, 16 mars 2006, portant adoption d'une norme simplifiée concernant les traitements automatisés de données à caractère personnel mis en œuvre par les organismes publics ou privés destinés à géolocaliser les véhicules utilisés par leurs employés (norme simplifiée no 51), *JO* n^o 1003, 3 mai — Rapp. présenté au ministre délégué à l'Emploi, au Travail et à l'Insertion professionnelle des jeunes, 7 mars 2007, *Charte d'éthique, alerte professionnelle et droit du travail français : état des lieux et perspectives,* sous http://lesrapports.ladocumentationfrancaise.fr/BRP/074000335/0000.pdf l

33.02

Jurisprudence de référence.

> Principe de prohibition des écoutes téléphonique sur les lieux de travail.

• **Soc. 7 nov.1995,** n^o 92-44.498, NPB, Sté polyclinique Volney c/M. Bordeau — confirmation **CA Rennes, 5^e ch., 29 sept. 1992**.

• **Soc. 3 févr. 1999,** n^o 97-40.495, NPB, Sté Locamion c/Belgacem ben Mariem — confirmation **CA Lyon, ch. soc. coll. B, 5 déc. 1996**.

• **Soc. 30 mars 1999,** n^o 97-40.850, NPB — confirmation **CA Lyon, ch. soc. coll. B, 8 nov. 1996**.

• **Soc. 18 nov.1998,** n^o 96-43.902, Sté Cegeor, SARL c/Mme I. NPB — confirmation **CA Lyon, ch. soc., 5 juin 1996**.

* V. s^s n^o 33.13.

> Sur le principe d'inviolabilité de la correspondance privée.

• **TGI Paris, 12^e ch., 1^er juin 2007,** Oddo et Cie c/Trinh Nghia T… et Trung T…, http://www.legalis.net/breves-article.php3?id_article=2178.

* V. s^s n^o 33.20.

> Sur la consultation de la messagerie et des fichiers créés par l'employé.

• **Soc. 2 oct. 2001, arrêt Nikon,** n^o 99-42.942, *Bull. civ.* V, n^o 291 ; *D.* 8 nov. 2001, n^o 39, jur., comm. 3148-3153 ; *Sem. soc. Lamy* 15 oct. 2001, n^o 1046 ; *JCP E et A* 29 nov. 2001, n^o 48, p. 1918-1922, note C. Puigelier ; *JCP G* n^o 2, 9 janv. 2002, doctr., I, 102, p. 63-69, note M. Bourrié-Quenillet et F. Rodhain ; *RTD civ.* janv.-mars 2002, n^o 1, 72-73, note J. Hauser ; *RJPF* janv. 2002, n^o 1, p. 10-11, note B. Bossu ; *RJS* n^o 12/01, déc. 2001, chron. p. 940-946, note F. Favennec-Hery ; *Gaz. Pal.* 16 mai 2002, n^o 136, p. 47, note H. Vray ; *LPA* 10 déc. 2001, n^o 245, p. 6, note G. Picca — cassation de **CA Paris, 18^e ch., sect. A, 22 sept. 1999**.

* V. s^s n^o 33.21.

• **Soc. 18 oct. 2006,** n^o 04-48.025, NPB, Jérémy L. F… c/Techni-Soft : *Bull. civ.* V,

18 oct. 2006 comm. Ray J.-E., L'envers de l'arrêt Nikon, *Sem. soc. Lamy* 2006, n° 1280, p. 10 ; P. Alix, « L'accès par l'employeur aux fichiers personnels stockés sur l'ordinateur du salarié », *JSL* n° 189-1, p. 4 ; J.-E. Tourreil, « Les documents détenus par un salarié dans l'entreprise sont présumés avoir un caractère professionnel », *JSL* n° 200, p. 15 v. http://www.legalis.net/jurisprudence-decision.php3?id_article=1774 ; *LPA* 28 avr. 2008, n° 85, p. 7, note X. Daverat et S. Tournaux — confirmation de **CA Rennes, ch. soc., 21 oct. 2004,** *Gaz. Pal.* 18 janv. 2007, n° 18, p. 37, note S. Hadjali et C. Fagot ; *LPA* 28 avr. 2008, n° 85, p. 7, note X. Daverat.

• **CA Toulouse, 4e ch. soc., 6 févr. 2003,** aff. n° 02-02519.

* V. s° 33.22, 33.21 et égalt n° 31.24.

• **Soc. 17 mai 2005,** n° 03-40.017, NPB, Philippe K… c/Sté Cathnet-Science, *Juris-Data* n° 028449 ; *CCE* juill.-août 2005, p. 34 s., comm. A. Lepage ; *Gaz. Pal.* 20 oct. 2005, n° 293, p. 36, note S. Hadjali ; *LPA* 23 avr. 2007, n° 81, p. 6, note S. Tournaux — cassation de **CA Paris, 22e ch., sect. A, 6 nov. 2002**.

• **CA Besançon, ch. soc., 21 sept. 2004,** RG n° 2003-1807, SNC General Electric Energy Products France c/Girardot et a., *RJS* 4/2005, n° 342.

• **Soc. 23 mai 2007,** n° 05-17.818, Datacep c/Hansart, NPB, *Bull. civ.* V ; *D.* 2007, AJ 1590, note A. Fabre ; *Gaz. Pal.* 18 mars 2008, n° 78, p. 20 ; *LPA* 28 avr. 2008, n° 85, p. 7, note X. Daverat et S. Tournaux — cassation de **CA Douai, 1re ch., sect. 2, 18 mai 2005**.

* V. s° 33.23.

• **CA Versailles, 2 avr. 2003,** aff. n° 02-00293 et **CA Besançon, ch. soc., 21 sept. 2004,** RG n° 2003-1807**,** SNC General Electric Energy Products France c/Girardot a., *RJS* 4/05, n° 342.

* V. s° 33.21.

> Sur le caractère « justifié et proportionné » d'un dispositif de contrôle.

• **Soc. 26 nov. 2002,** n° 00-42.401, Montaigu Meret c/ Wieth Lederle, NPB, *Bull. civ.* V, n° 352 ; *RTD civ.* 2003, 58 ; *Gaz. Pal.* 1er févr. 2003, n° 32, p. 23, note C.-E. Brault : au sujet de la géolocalisation — cassation de **CA Nancy, ch. soc., 23 févr. 2000**.

* V. s° 33.31.

• **TGI Paris, 19 avr. 2005,** *CCE* oct. 2005, comm. 164, p. 46.

* V. s° 33.11.

• **TGI Paris, 1re ch., 19 avr. 2005,** CE Effia Services, Synd. Sud Rail c/Effia Services, *CCE* oct. 2005, p. 46 s, http://www.legalis.net/breves-article.php3?id_article=1434.

* V. s° 33.11

> Sur le Caractère présumé privé ou professionnel d'un message ou d'un fichier.

• **Soc. 18 oct. 2006,** n° 04-48.025, NPB, Jérémy L. F… c/Techni-Soft (préc.) — confirmation de **CA Rennes, ch. soc., 21 oct. 2004** (préc.).

• **CA Bordeaux, ch. soc., sect. A, 8 févr. 2005,** n° 04/02449.

* V. s° 33.22.

> Sur les dispositifs d'alerte professionnelle.

• **TGI Libourne, ord. réf., 15 sept. 2005,** RG n° 05/00143, Comité d'établissement BSN Glasspack, Synd. CGT du personnel de BSN Glasspack c/SAS BSN-Glasspack, v. chron. F. Naftalski, *Lamy Dr. informatique et réseaux* 2005 : retrait.

• **TGI Nanterre, ord. réf., 27 déc. 2006 :** suspension du dispositif.

• ***CONTRA :*** pour le maintien du dispositif, **TGI Lyon, ch. urg., 19 sept. 2006**, Union départementale CGT du Rhône, synd. CGT Bayer Cropscience c/Bayer Cropscience.

• **TGI Nanterre, ord. réf., 1er avr. 2005,** CE ING Bank c/ING Bank France.

* V. s° 33.32.

33.03

Bibliographie indicative.

> Guides.

Cnil, *Guide pratique pour les employeurs* — Communication de la CNIL relative à la mise en oeuvre de dispositifs de reconnaissance par empreinte digitale avec stockage dans une base de données, v. http://www.cnil.fr/index.php?id=2363&news[uid]=508&cHash=0a2ef80a3e.

> Articles.

G. Haas et L. Goutorbe, « Cybersurveillance : l'employeur doit être prudent en matière de collecte de preuve », *Expertises* août-sept. 2005, p. 304 — R. de Quenaudon, « Liberté et sécurité dans l'entreprise : une conciliation de plus en plus problématique », *RDT* 2006, p. 395 ; « Quelques remarques à propos de connexions illicites du salarié », *RDT* 2007,

p. 370.

33.04

Questions principales.

• Comment concilier le droit de contrôle de l'employeur sur l'outil de travail et le respect de la vie privée de l'employé ?

* V. s^s n^o 33.11.

• À quelles conditions peut-on accéder aux données personnelles d'un employé ?

* V. s^s n^os 33.20 s.

• Quels sont les critères d'appréciation pour obtenir une autorisation de contrôle biométrique d'accès sur les lieux du travail ?

* V. s^s n^o 33.30, égalt n^os 28.00 s.

SECTION 1
UN DISPOSITIF JUSTIFIE

33.11

Un dispositif de contrôle « justifié ». La loi du 31 décembre 1992 a instauré un « principe de proportionnalité », désormais inséré à l'article L. 1121-1 du Code du travail : « Nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives de restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché » (anc^t art. L. 120-2).

C'est ce qu'a rappelé le tribunal de grande instance de Paris, dans sa décision du 19 avril 2005[39], à propos d'un dispositif biométrique, dont la mise en œuvre était contestée judiciairement par le comité d'entreprise et le syndicat Sud-Rail. Ces derniers considéraient que le système de lecture d'empreintes digitales pour gérer et contrôler le temps de présence des employés sur divers sites de travail portait atteinte aux droits et libertés individuelles des employés.

L'employeur ne peut ainsi exercer un contrôle que lorsqu'il est confronté à un comportement suspect de son employé : des délais de connexion anormalement longs ou encore des opérations de téléchargement anormalement lourdes (connexion et téléchargement de jeux ou encore d'images pornographiques) pourraient par exemple constituer des indices justifiant une mesure de surveillance et d'interception. À noter toutefois que de telles vérifications pourraient être considérées comme une « entrave » s'il s'agit d'un employé « protégé » (délégué syndical, délégué du personnel, membre du comité d'entreprise, *etc.*).

33.12

Encadrement juridique des autocommutateurs. Dans une première recommandation du 18 septembre 1984, la Commission nationale de l'informatique et des libertés (Cnil) précisait que l'employeur ne peut pas enregistrer les conversations téléphoniques, ni l'intégralité des numéros de téléphone appelés par ses employés (mais seulement les quatre premiers numéros, pour savoir si l'employé a appelé l'étranger ou la province, *etc.*[40]) ;

Depuis, par délibération du 20 décembre 1994, la Cnil a élaboré une norme simplifiée constituant l'encadrement juridique de l'usage des autocommutateurs. Ce dispositif permet de conserver en mémoire les numéros de téléphone composés par les employés, depuis leur poste de travail. Il a clairement été établi par la Commission que l'utilisation des lignes téléphoniques par les employés à des fins privées était permise, l'employeur pouvant toutefois exiger des employés concernés le remboursement des communications répondant à de telles fins. Cependant, si l'employeur dispose de la possibilité de conserver les numéros de téléphone composés par les employés depuis leur poste de travail, ces numéros ne peuvent en aucun cas être divulgués intégralement à d'autres employés. L'employeur ne peut, en outre, conserver ces numéros pendant une durée

---

[39] TGI Paris, 1re ch., 19 avr. 2005, CE Effia Services, Synd. Sud Rail c/Effia Services, *CCE* oct. 2005, p. 46 s.

[40] Cnil, recomm. n° 84-31, 18 sept. 1984, concernant l'usage des autocommutateurs téléphoniques sur les lieux de travail, *3e Rapport d'activités de la Cnil,* Doc. fr., p. 109, http://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000017654576&fastReqId=227990&fastPos=1.

excédant six mois. Enfin, la Cnil rappelle que les représentants du personnel doivent être consultés avant la mise en place d'un tel système d'autocommutateur.

33.13

Conditions d'interception des communications passées par les employés. La pratique des écoutes téléphoniques a été réglementée par la loi du 17 juillet 1970. Elle a été complétée par la loi du 10 juillet 1991 qui élargit la portée du principe de prohibition des écoutes téléphoniques. Elle insère ainsi, dans le Code pénal, un article 226-15 alinéa 2 qui incrimine « le fait, commis de mauvaise foi, d'intercepter, de détourner, d'utiliser ou de divulguer des correspondances émises, transmises ou reçues par la voie des télécommunications ou de procéder à l'installation d'appareils conçus pour réaliser de telles interceptions » (un an d'emprisonnement et 45 000 euros d'amende).

Est puni des mêmes peines, le fait, commis de mauvaise foi, d'ouvrir, de supprimer, de retarder ou de retourner des correspondances arrivées ou non à destination et d'en prendre connaissance frauduleusement (C. pén., art. 226-15, al. 1).

L'article 432-9 du Code pénal incrimine également le fait, pour une personne dépositaire de l'autorité publique ou chargée d'une mission de service public, d'ordonner, de commettre, ou de faciliter, hors les cas prévus par la loi, l'interception ou le détournement des correspondances émises, transmises ou reçues par la voie des télécommunications, l'utilisation ou la divulgation de leur contenu (trois ans d'emprisonnement, 45 000 euros d'amende).

De surcroît, le Code pénal subordonne la détention d'appareils conçus pour réaliser de telles interceptions à l'octroi d'une autorisation délivrée par une commission, spécialement instituée à cet effet par l'article R. 226-2 du même code, et présidée par le secrétariat général de la Défense nationale.

Un doute demeurait quant à l'application de cette interdiction aux employeurs. La Cnil a autorisé l'employeur à intercepter les communications passées par les employés de l'entreprise, à condition que la finalité du dispositif d'écoutes soit précisée, que les employés soient prévenus de la mise en place d'un tel dispositif, préalablement à son installation, des conséquences possibles de l'interception de communications, des périodes durant lesquelles leurs conversations pourront être enregistrées. De plus, il est prévu que les employés puissent bénéficier de lignes non connectées au dispositif d'écoute pour toutes les conversations qui ne sont pas directement liées au motif de l'écoute. Enfin, il est précisé que lorsque l'écoute est opérée à des fins de contrôle de qualité de la réponse téléphonique, les employés doivent pouvoir avoir connaissance à bref délai du compte rendu de la conversation enregistrée. Les enregistrements doivent ensuite être effacés, une fois l'analyse effectuée, dans un délai de l'ordre de quinze jours à un mois. D'autre part, les clients appelants doivent être informés de l'enregistrement de leur appel.

La jurisprudence a consacré certains principes en matière d'écoutes téléphoniques. En effet, l'utilisation à des fins personnelles de la ligne téléphonique professionnelle a été jugée, dans de nombreuses affaires, constitutive d'une faute grave[41]. Mais d'autres arrêts ont reconnu qu'une telle utilisation, si elle n'était pas constitutive d'une faute grave, était susceptible de constituer une cause réelle et sérieuse de licenciement[42]. Toutefois, la jurisprudence a également considéré que les licenciements prononcés pour ce motif étaient injustifiés, lorsqu'ils paraissaient disproportionnés aux faits de la cause[43].

---

[41] Soc. 7 nov. 1995, n° 92-44.498, NPB, sté polyclinique Volney c/M. Bordeau ; v. http://www.legifrance.gouv.fr/affichJuriJudi.do?oldAction=rechJuriJudi&idTexte=JURITEXT000007286836.

[42] Soc. 3 févr. 1999, n° 97-40.495, NPB, sté Locamion c/Belgacem ben Mariem, http://www.legifrance.gouv.fr/affichJuriJudi.do?oldAction=rechJuriJudi&idTexte=JURITEXT000007394923.

[43] Soc. 30 mars 1999, n° 97-40850 ; Soc. 18 nov. 1998, n° 96-43902, NPB, sté Cégéor c/Mme I. Maulet, v. http://www.legifrance.gouv.fr/affichJuriJudi.do?oldAction=rechJuriJudi&idTexte=JURITEXT000007399898.

On retiendra donc que les seules dérogations admises concernent les activités de marketing téléphonique, de vente par correspondance, de standard, afin de permettre à l'employeur de contrôler le travail. À défaut d'une nécessité reconnue et proportionnée, une solution alternative devra être recherchée, par exemple « plutôt qu'enregistrer toutes les conversations avec la clientèle à des fins de constitution de preuves matérielles pour faire face à un éventuel contentieux, demander une confirmation écrite au client, notamment par voie électronique »[44].

SECTION 2
CONDITIONS D'ACCES AUX DONNEES PERSONNELLES DE L'EMPLOYE

33.21

Principe de l'inviolabilité des correspondances. Toute violation de ce principe constitue l'infraction visée et réprimée par l'article 226-15 du Code pénal : « Le fait, commis de mauvaise foi, d'ouvrir, de supprimer, de retarder ou de détourner des correspondances arrivées ou non à destination et adressées à des tiers, ou d'en prendre frauduleusement connaissance, est puni d'un an d'emprisonnement et de 45 000 euros d'amende. Est puni des mêmes peines le fait, commis de mauvaise foi, d'intercepter, de détourner, d'utiliser ou de divulguer des correspondances émises, transmises ou reçues par la voie des télécommunications ou de procéder à l'installation d'appareils conçus pour réaliser de telles interceptions »[45].

Plusieurs décisions rappellent ainsi l'interdiction faite à l'employeur de prendre connaissance des messages personnels émis et reçus par ses employés. L'arrêt de la Cour de cassation du 2 octobre 2001 (arrêt Nikon[46]) précise tout particulièrement que « le salarié a droit, même au temps et au lieu de travail, au respect de l'intimité de sa vie privée ; que celle-ci implique en particulier le secret des correspondances ; que l'employeur ne peut dès lors, sans violation de cette liberté fondamentale, prendre connaissance des messages personnels émis par le salarié et reçus par lui grâce à un outil informatique mis à sa disposition pour son travail et ceci même au cas où l'employeur aurait interdit une utilisation non professionnelle de l'ordinateur ». Dans cette affaire, l'employeur avait découvert que son employé entretenait une activité parallèle qu'il développait pendant ses heures de travail et à partir de son poste informatique mis à sa disposition par l'entreprise qui l'employait. Les éléments de preuve collectés dans la messagerie de l'employé ont été obtenus, selon les juges, de façon illicite et, à ce titre, ont été écartés des débats.

Plus récemment, la Cour de cassation a approuvé un arrêt de la cour d'appel qui, relevant le caractère privé du courrier électronique adressé par l'employé à l'un de ses collègues de travail, en a déduit que cet élément de la vie personnelle de l'interessé ne pouvait constituer un motif de licenciement[47].

Le principe de l'inviolabilité de la correspondance s'applique également aux employés comme l'illustre ce jugement du tribunal de grande instance de Paris (TGI Paris, 1er juin 2007[48]) qui a condamné un ancien consultant informatique

---

[44] Cnil, *Guide pratique pour les employeurs,* p. 21, http://www.cnil.fr/fileadmin/documents/La_CNIL/publications/CNIL_GuideTravail.pdf.

[45] Cet article est issu de l'ordonnance n° 2000-916, 19 sept. 2000, art. 3, *JO* 22 sept. 2000, en vigueur le 1er janvier 2002.

[46] Soc. 2 oct. 2001, n° 99-42.942, Nikon France c/M. Onof, cass. CA Paris, 22 mars 1999 (renvoi devant la CA Paris autrement composée), *D.* 2001, 3148, note P.-Y. Gautier ; *D.* 2002, somm. 2296, note C. Caron ; *CCE* 2001, comm. 120 et obs. ; *Dr. soc.* nov. 2001, p. 915, note J.-E. Ray — v. aussi débat autour de l'arrêt Nikon France, n° 99-42.942, *Bull. civ.* V, n° 291 ; *Sem. soc. Lamy* 15 oct. 2001, n° 1046, http://www.legifrance.gouv.fr/WAspad/UnDocument?base=CASS&nod=CXCXAX2001X10X05X00291X000 ; *Gaz. Pal.*, 16 mai 2002, n° 136, p. 47, note H. Vray ; *LPA*, 10 déc. 2001, n° 245, p. 6, note G. Picca.

[47] Soc. 6 juin 2007, n° 05-43.996, NPB, sté Eliophot c/M. X…. : rejet du pourvoi contre CA Aix-en-Provence, 18e ch., 7 juin 2005.

[48] TGI Paris, 1er juin 2007, Oddo et Cie c/Trinh Nghia T… et Trung T…, consultable sur le site legalis.net : http://www.legalis.net/jurisprudence-decision.php3?id_article=2179.

d'une société qui avait conservé, bien après son départ, les codes lui permettant d'accéder aux messageries électroniques du directeur général et du directeur des ressources humaines. Dans cette affaire, les deux dirigeants avaient découvert qu'ils faisaient l'objet d'une surveillance électronique. La perquisition effectuée chez le consultant a permis de constater des traces de connexions aux messageries concernées. Il a déclaré avoir transmis ces codes à son frère, ancien salarié de cette société, travaillant actuellement pour son concurrent, pour surveiller le rachat éventuel de la société Oddo par son employeur. Comme l'ont rappelé les juges, le simple fait de consulter les courriers électroniques de tiers en utilisant leurs codes d'accès constitue un accès frauduleux à un système informatique et une atteinte au secret des correspondances en violation de l'article 226-15 du Code pénal.

33.22

Messages présumés professionnels. Selon la Cnil, « il doit être généralement considéré qu'un message envoyé ou reçu depuis le poste du travail mis à disposition par l'entreprise ou l'administration revêt un caractère professionnel, sauf indication manifeste dans l'objet du message ou dans le nom du répertoire où il pourrait avoir été archivé par son destinataire qui lui conférerait alors le caractère et la nature d'une correspondance privée protégée par le secret des correspondances »[49].

C'est le raisonnement qui a été suivi par les juges de la cour d'appel de Bordeaux pour admettre les preuves produites par l'employeur. Ils ont en effet précisé que « les dossiers et fichiers présents sur l'ordinateur des salariés, ou encore les documents qu'ils détiennent dans leur bureau, ont nécessairement un caractère professionnel quand ils ne les ont pas identifiés comme personnels. Il en résulte que l'employeur a légitimement accès à ces dossiers, fichiers ou documents professionnels, sans qu'il soit nécessaire que le salarié concerné soit présent. Par conséquent, les ordinateurs des salariés sont accessibles par l'employeur. Donc, (l'employeur) pouvait en toute légalité avoir accès à l'ordinateur de (l'employée). En l'absence de mention particulière apportée (par l'employée) aux mails qu'elle a envoyés de son ordinateur professionnel […], (l'employeur) est en droit de les produire en justice. En conséquence, l'existence des mails est reconnue et les faits sont donc bien établis » (CA Bordeaux, ch. soc., sect. A, 8 févr. 2005[50]).

Dans cette logique, *a contrario,* dès lors que l'objet d'un message indique le caractère privé de ce dernier, l'employeur ne peut en principe ouvrir ce message afin d'en lire le contenu.

Cependant, d'autres décisions rappellent que la règle de l'inviolabilité s'applique en toutes circonstances, même lorsque l'objet du message n'est pas explicite, à charge pour l'employeur de vérifier les éléments susceptibles de conférer audit message un caractère manifestement personnel (tel serait le cas d'un message dont l'objet concerne les vacances et qui est classé dans un dossier portant la mention « personnel »)[51].

Aussi, pour faire échec à cette règle, les employeurs ont recours à différents moyens, notamment l'insertion de dispositions spécifiques dans la charte relative à l'utilisation des outils informatique. À titre d'exemple, on peut citer ce jugement du 15 septembre 2005 du Conseil des prud'hommes de Nanterre. Dans cette affaire, un salarié, qui faisait parvenir de nombreux messages à une société concurrente, avait été licencié pour faute grave. Les conseillers ont considéré que, bien que comportant la mention « message strictement privé et confidentiel », il n'y avait pas lieu de faire droit à la demande du requérant qui sollicitait la déclaration d'un licenciement privé de cause réelle et sérieuse, au motif que la « charte des moyens de communication », mis en place au sein de l'entreprise, complément du règlement intérieur, précisait que « les messages à caractère privé doivent porter la mention PRV ». De ce fait, l'employeur était totalement libre de prendre

[49] Cnil, *Guide pratique pour les employeurs.*

[50] CA Bordeaux, ch. soc., sect. A, 8 févr. 2005, n° 04/02449.

[51] CA Toulouse, 4e ch. soc., 6 févr. 2003, aff. n° 02-02519.

connaissance de tout message ne comportant pas une telle mention.

33.23
Accès aux fichiers personnels en présence de l'employé. La cour d'appel de Besançon a considéré que la violation du secret de la correspondance privée ne pouvait être invoquée, l'employeur n'ayant pas directement accédé aux fichiers en cause (à caractère pornographique), leur ouverture et leur lecture ayant été effectuées par un expert judiciaire missionné par le conseil de prud'hommes en présence des parties ou de leurs conseils (CA Besançon, 24 sept. 2004[52]). La Cour de cassation a confirmé que l'employeur pouvait avoir accès aux fichiers personnels d'un salarié. Dans cette affaire, l'employeur avait découvert des photos érotiques dans le tiroir du bureau de son employé et avait alors décidé d'investiguer le disque dur de l'ordinateur de celui-ci. Un fichier dénommé « perso » regroupait une série de documents étrangers aux fonctions de l'employé. Selon la Cour, « sauf risque ou évènement particulier, l'employeur ne peut ouvrir les fichiers identifiés par la salarié comme personnels contenus sur le disque dur de l'ordinateur mis à sa disposition qu'en présence de ce dernier ou celui-ci dûment appelé » (Soc. 17 mai 2005[53]). Depuis, la Haute juridiction a précisé que « les dossiers et fichiers créés par un salarié grâce à l'outil informatique mis à sa disposition par son employeur pour l'exécution de son travail, sont présumés, sauf si le salarié les identifie comme étant personnels, avoir un caractère professionnel de sorte que l'employeur peut y avoir accès hors sa présence » (Soc. 18 oct. 2006[54]).

Dans cette même logique, la cour d'appel de Versailles a écarté les messages produits par un employeur pour démontrer que son employé créait une société concurrente car ceux-ci avaient été récupérés sur l'ordinateur portable de l'employé sans satisfaire à la demande préalable de ce dernier de se voir restituer ses fichiers personnels (CA Versailles, 2 avr. 2003[55]).

33.23
Production des SMS à titre de preuve. La Cour de cassation a eu à se prononcer sur la recevabilité de SMS à titre de preuve dans une affaire dans laquelle l'employée, licenciée pour faute grave, contestait son licenciement, invoquant le harcèlement sexuel dont elle avait fait l'objet. Ces faits, établis par SMS, ont été admis par la cour d'appel. L'employeur a formé un pourvoi en cassation, constestant la recevabilité des éléments de preuves produits (des messages téléphoniques reconstitués et retranscrits par un huissier à l'insu de leur auteur et un entretien enregistré par la salariée sur une microcassette à l'insu de l'employeur). La Cour de cassation a considéré que si l'enregistrement d'une conversation téléphonique privée, effectuée à l'insu de l'auteur des propos est effectivement un procédé déloyal rendant irrecevable en justice la preuve ainsi obtenue, il n'en est pas de même de l'utilisation par le destinataire des SMS dont l'auteur ne peut ignorer qu'ils sont enregistrés par l'appareil récepteur. Les SMS établissaient donc bien la preuve du harcèlement sexuel dont se plaignait l'employée (Soc. 23 mai 2007[56]).

---

[52] CA Besançon, ch. soc., 21 sept. 2004, RG n° 2003-1807, SNC General Electric Energy Products France c/Girardot et a., *RJS* 4/2005, n° 342.

[53] Soc. 17 mai 2005, n° 03-40.017, NPB, Philippe X. c/Cabinet-Science, *Juris-Data* n° 2005-028449 ; *CCE* juill.-août 2005, p. 34 s., comm. A. Lepage ; v. aussi G. Haas et L. Goutorbe, « Cybersurveillance : l'employeur doit être prudent en matière de collecte de preuve », Expertises août-sept. 2005, p. 304 ; *Gaz. Pal.*, 20 oct. 2005, n° 293, p. 36, note S. Hadjali ; *LPA* 23 avr. 2007, n° 81, p. 6, note S. Tournaux

[54] Soc. 18 oct. 2006, n° 04-48.025, Jérémy L. F… c/Techni-Soft, *Bull. civ.* V, 18 oct. 2006, comm. J.-E. Ray, L'envers de l'arrêt Nikon, *Sem. soc. Lamy* 2006, n° 1280, p. 10 ; P. Alix, « L'accès par l'employeur aux fichiers personnels stockés sur l'ordinateur du salarié », *JSL* n° 189-1, p. 4 ; J.-E. Tourreil, « Les documents détenus par un salarié dans l'entreprise sont présumés avoir un caractère professionnel », *JSL* n° 200, p. 15, v. http://www.legalis.net/jurisprudence-decision.php3?id_article=1774 ; *Gaz. Pal.* 18 janv. 2007, n° 18, p. 37, note S. Hadjali et C. Fagot ; *LPA* 28 avr. 2008, n° 85, p. 7, note X. Daverat.

[55] CA Versailles, 2 avr. 2003, aff. n° 02-00293.

[56] Soc. 23 mai 2007, n° 05-17.818, NPB, *Bull. civ.* V ; *D.* 2007, AJ 1590, note A. Fabre ; *Gaz. Pal.*

SECTION 3

UN DISPOSITIF SENSIBLE

33.30

Contrôle d'accès biométrique. On observe un développement important des dispositifs biométriques ayant pour objet le contrôle des accès sur le lieu du travail ou à des systèmes d'information (v. s^{s} n^{os} 28.20 s.).

Leur mise en œuvre est subordonnée à une autorisation délivrée par la Cnil. Celle-ci précise, dans un guide rendu public le 28 décembre 2007[57], ses principaux critères d'appréciation ainsi que les risques auxquels s'exposent les entreprises qui y ont recours et les droits des employés (v. s^{s} n^{os} 28.21 s.).

Pour l'essentiel, le dispositif doit répondre à un « fort impératif de sécurité ». Par ailleurs, la finalité du dispositif doit être limité au contrôle de l'accès à une zone bien définie pour un nombre déterminé de personnes (1er critère). À raison des risques associés pour la protection des données à caractère personnel, le dispositif doit être « proportionné », c'est-à-dire adapté à la finalité qu'il poursuit (2^{e} critère). Des garanties doivent être prises pour que l'authentification et/ou l'identification ne provoquent pas la divulgation des données (3^{e} critère). Enfin, les personnes concernées doivent être informées (4^{e} critère).

La Cnil a ainsi autorisé, le 13 septembre 2007[58], la mise en œuvre d'un traitement automatisé de données à caractère personnel reposant sur un procédé de reconnaissance vocale. Ce dispositif qui vise à permettre de générer et de réinitialiser automatiquement les mots de passe d'accès au système d'information de l'entreprise, repose sur la reconnaissance du gabarit de l'empreinte de la voix des employés.

La Cnil a également autorisé, le 8 novembre 2008, par cinq délibérations (n^{o} 2007-335 à n^{o} 2007-339)[59], la mise en œuvre de plusieurs dispositifs reposant sur la reconnaissance du réseau veineux du doigt de la main et ayant pour objet le contrôle de l'accès aux locaux ou à des systèmes d'information.

33.31

Géolocalisation. De plus en plus d'entreprises mettent en œuvre des dispositifs de géolocalisation qui permettent d'identifier la position géographique, à un instant donné ou en continu, de leurs employés, par la localisation de matériels dont ils ont l'usage, notamment les véhicules qui leurs sont confiés par leur employé. Ces dispositifs sont principalement basés sur l'utilisation de la technologie GSM/GPS qui permet de localiser à chaque instant la position d'un véhicule équipé d'un tel système. Les traitements résultant de ces dispositifs permettent de collecter des données telles que la durée d'utilisation du véhicule, le kilométrage parcouru ou les vitesses de circulation.

La Cnil considère que cette « mise sous surveillance permanente des déplacements des salariés est disproportionnée lorsque la tâche à accomplir ne réside pas dans le déplacement lui-même mais dans la réalisation d'une prestation pouvant faire elle-même l'objet d'une vérification »[60]. La Cour de cassation, dans un arrêt du 26 novembre 2002[61], a ainsi considéré qu'« une filature organisée par l'employeur pour contrôler et surveiller l'activité d'un salarié constitue un moyen de preuve illicite, sans faire de distinction selon que le salarié a été ou non informé de l'existence d'un tel contrôle »[62]. Aussi, la Cnil a-t-elle entrepris de lancer une consultation auprès des acteurs concernés, notamment des ministères, des organisations syndicales et professionnelles et des intégrateurs de services de

---

18 mars 2008, n^{o} 78, p. 20 ; *LPA* 28 avr. 2008, n^{o} 85, p. 7, note X. Daverat et S. Tournaux.

[57] http://www.cnil.fr/fileadmin/documents/approfondir/dossier/CNI-biometrie/Communication-biometrie.pdf.

[58] Cnil, délib. n^{o} 2007-248, 13 sept. 2007, http://www.wk-rh.fr/mybdd/upload/bdd_80/Cnil-D2007-248.pdf.

[59] Cnil, délib. n^{os} 2007-335 à 2007-339, 8 nov. 2007, http://www.wk-rh.fr/mybdd/upload/bdd_80/Cnil-D2007-335-339.pdf.

[60] Cnil, *Guide pratique pour les employeurs,* p. 23.

[61] Soc. 26 nov. 2002, n^{o} 00-42.401, *Bull. civ.* V, n^{o} 352 ; *RTD civ.* 2003, 58.

[62] Cnil, *Guide pratique pour les employeurs,* p. 23.

géolocalisation, afin de bien encadrer les conditions d'utilisation de ces dispositifs[63].

Cette réflexion a mené à l'adoption, le 16 mars 2006, de deux délibérations n° 2006-066 et n° 2006-067 portant respectivement recommandation et norme simplifiée « concernant les traitements automatisés de données à caractère personnel mis en œuvre par les organes publics ou privés destinés à géolocaliser les véhicules utilisés par leurs employés »[64]. Compte tenu du caractère intrusif de la mise en place de dispositifs de géolocalisation, la Cnil dresse une liste des finalités pour lesquelles l'insertion d'un tel dispositif lui semble légitime et est donc admissible (sûreté ou sécurité de l'employé ou des marchandises, meilleure allocation des moyens, suivi et facturation d'une prestation de transport de personnes ou de marchandises ou d'une prestation de service directement liée à l'utilisation du véhicule, suivi du temps de travail). D'autre part, la commission indique que l'utilisation d'un tel dispositif ne doit pas conduire à un contrôle permanent de l'employé concerné. Elle prévoit un allègement considérable des formalités administratives pour les entreprises se conformant aux conditions envisagées, notamment quant aux types de données collectées et à la durée de leur conservation (norme simplifiée n° 51). Cette délibération dresse, à ce titre, une liste de finalités auxquelles doit impérativement répondre la collecte d'informations par un tel procédé. La Cnil délimite également les données qui peuvent être traitées, par la mise en place d'un dispositif de géolocalisation. Elle établit aussi une liste limitative des destinataires de ces données.

Enfin, la Cnil précise que les responsables de traitement, souhaitant mettre en place un dispositif de géolocalisation, doivent nécessairement procéder à l'information et à la consultation des instances représentatives du personnel, avant l'établissement d'un tel dispositif. Ce devoir d'information est également dû à l'égard des employés soumis à ce dispositif. D'autre part, les responsables de traitement doivent s'assurer que toutes les mesures de sécurité nécessaires ont été prises.

33.32

Dispositifs d'alerte professionnelle. La loi américaine Sarbanes-Oxley (juillet 2002) impose aux sociétés cotées aux États-Unis et à leurs filiales étrangères de procurer à leurs employés un dispositif de *whistleblowing* (dénommé, en français, « alerte professionnelle » ou encore « alerte éthique ») qui doit permettre de dénoncer les délits financiers dont ils ont connaissance.

Il n'existe pas de loi française sur ces dispositifs mais elle pourrait bien voir le jour, cette voie étant préconisée par un rapport remis le 7 mars 2007[65] au ministre délégué à l'Emploi, au Travail et à l'Insertion professionnelle des jeunes. En effet, ce rapport, dénommé *Charte d'éthique, alerte professionnelle et droit du travail français : état des lieux et perspectives,* préconise plusieurs voies pour renforcer la sécurité juridique des chartes d'éthique et pour encadrer un système d'alerte professionnelle. Il propose notamment d'introduire dans le Code du travail des règles spécifiques pour permettre aux entreprises de mettre en place des dispositifs organisant la possibilité de signaler, non seulement des actes contraires aux dispositifs législatifs ou réglementaires et des atteintes aux droits des personnes et à la santé des salariés, mais également des actes contraires à des règles d'origine éthique ou professionnelle. Ainsi, cette nouvelle règlementation aurait essentiellement pour objectifs de « – définir l'alerte professionnelle ; – déterminer les instruments juridiques de mise en place du dispositif ; – fixer les règles d'organisation que doit contenir l'instrument juridique choisi ; – protéger l'émetteur ».

Pour l'heure, c'est la Cnil qui encadre les conditions de mise en oeuvre de ces dispositifs qu'elle définit comme des « systèmes mis à la disposition des employés

---

[63] Cnil, communiqué 29 sept. 2005.

[64] Cnil, délib. n° 2006-067, 16 mars 2006, portant adoption d'une norme simplifiée concernant les traitements automatisés de données à caractère personnel mis en œuvre par les organismes publics ou privés destinés à géolocaliser les véhicules utilisés par leurs employés (norme simplifiée n° 51), *JO* n° 1003, 3 mai.

[65] V. le rapport *Charte d'éthique, alerte professionnelle et droit du travail français : état des lieux et perspectives,* sous http://lesrapports.ladocumentationfrancaise.fr/BRP/074000335/0000.pdf l.

d'un organisme public ou privé pour les inciter, en complément des modes normaux d'alerte sur les dysfonctionnements de l'organisme, à signaler à leur employeur des comportements qu'ils estiment contraires aux règles applicables et pour organiser la vérification de l'alerte ainsi recueillie au sein de l'organisme concerné ».

Dans un premier temps, la Cnil avait refusé, en mai 2005[66], d'autoriser la mise en œuvre de tels dispositifs, considérant qu'ils « étaient disproportionnés au regard des objectifs poursuivis et des risques de dénonciations calomnieuses et de stigmatisation des employés objets d'une alerte éthique ». Elle a également souligné que « les employés concernés par un signalement ne seraient, par définition, pas informés dès l'enregistrement de données mettant en cause leur intégrité professionnelle ou de citoyen et n'auraient donc pas les moyens de s'opposer à ce traitement de données les concernant. Les modalités de collecte et de traitement de ces données, dont certaines pouvaient concerner des faits susceptibles d'être constitutifs d'infractions pénales, peuvent donc être qualifiées de déloyales ». Cette position a eu pour effet de mettre les filiales françaises d'entreprises américaines en difficulté, celles-ci étant tenues de respecter les dispositions contradictoires de la loi informatique et libertés et celles de la loi *Sarbanes-Oxley.*

Aussi, la Cnil a-t-elle révisé sa position. Elle s'est d'abord rapprochée de la *Securities and Exchange Commission (SEC)* en vue de trouver des garanties compatibles tant avec la loi informatique et libertés qu'avec la loi *Sarbanes-Oxley* et a publié le 10 novembre 2005[67] un document d'orientation pour préciser les conditions dans lesquelles il est possible de mettre en place un dispositif d'alerte éthique. Elle a ensuite adopté le 8 décembre 2005[68] une décision d'autorisation unique fixant les conditions à respecter pour pouvoir bénéficier des formalités simplifiées. Pour l'essentiel, elle a admis le principe de l'alerte professionnelle, mais en restreignant son champ à des domaines précis (comptable, financier, bancaire et de lutte contre la corruption). Par ailleurs, elle prévoit qu'un tel dispositif exige la mise en place de mesures de précaution pour collecter, traiter et transférer hors de l'Union européenne les données concernées. Parallèlement, les droits d'information, d'accès et de rectification des salariés ont été aménagés.

Le groupe G 29 (v. s^{s} n^{o} 15.18) a également adopté le 1er février 2006[69] un avis sur les dispositifs d'alerte professionnelle dans les domaines bancaire, comptable, du contrôle interne des comptes, d'audit et de lutte contre la corruption et les délais financiers. Il reprend pour l'essentiel les principes du document d'orientation et de l'autorisation unique émis par la Cnil en novembre et décembre 2005.

En marge de ces prescriptions, il faut tenir compte de la jurisprudence, à raison de l'inflation des actions visant à faire supprimer les systèmes d'alerte éthique. Ainsi, par ordonnance du 15 septembre 2005[70], le juge des référés du tribunal de Libourne (Gironde) a demandé à la filiale française d'une société américaine, de retirer son dispositif d'alerte éthique, considérant que cette mesure s'imposait à

---

[66] Cnil, délib. n^{o} 2005-110, 26 mai 2005, relative à une demande d'autorisation de Mc Donald's France pour la mise en œuvre d'un dispositif d'intégrité professionnelle, http://www.cnil.fr/index.php?id=1833&delib[uid]=73&cHash=ed7a84e6a7 — et Cnil, délib. n^{o} 2005-111, 26 mai 2005, relative à une demande d'autorisation de la Compagnie européenne d'accumulateurs pour la mise en œuvre d'un dispositif de ligne éthique, http://www.cnil.fr/index.php?id=1834&delib[uid]=74&cHash=89a931a002.

[67] Doc. d'orientation adopté par la Commission le 10 nov. 2005 pour la mise en œuvre de dispositifs d'alerte professionnelle conformes à la loi du 6 janvier 1978 modifiée en août 2004, relative à l'informatique, aux fichiers et aux libertés, http://www.cnil.fr/fileadmin/documents/La_CNIL/actualite/CNIL-docori-10112005.pdf.

[68] Cnil, délib. n^{o} 2005-305, 8 déc. 2005, portant autorisation unique de traitements de données à caractère personnel mis en œuvre dans le cadre de dispositifs d'alerte professionnelle, http://www.cnil.fr/index.php?id=1969.

[69] G 29, avis, 1er févr. 2006, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp117_en.pdf.

[70] TGI Libourne, 15 sept. 2005, BSN Glasspack, cité dans « Alertes éthiques : quelles orientations suite aux décisions de la CNIL ? », *RLDI* 2005/11, n^{o} 318, obs. F. Naftalkski ; *CCE* déc. 2005, A. Lepage, comm. 191, p. 37 et A. Caprioli, comm. 194, p. 44.

raison de « la seule existence d'un dommage potentiel imminent pour les libertés individuelles de salariés victimes de dénonciations anonymes recueillies par le biais d'un dispositif privé échappant à tout contrôle, sans que l'intérêt de l'entreprise ne permette sérieusement de le justifier ». Une ordonnance de référé du 27 décembre 2006 du tribunal de grande instance de Nanterre a également enjoint la suspension de la diffusion d'un questionnaire intitulé « business ethics » que les salariés avaient l'obligation de remplir et leur imposant notamment de « signaler si un membre de leur famille a un intérêt significatif dans une entreprise extérieure cherchant à travailler ou étant en concurrence avec la société » ou encore de préciser « si une relation familiale ou personnelle, pourrait les dissuader d'agir dans les meilleurs intérêts de la société »[71]. Le juge des référés a ainsi estimé que ce dispositif d'alerte éthique était non conforme à la délibération de la Cnil du 8 décembre 2005, en particulier dans la mesure où la Cnil a précisé que ne pourraient bénéficier du régime d'autorisation unique « que les dispositifs d'alerte ne présentant pas un caractère obligatoire ».

Mais il faut également compter avec les décisions validant les dispositifs d'alerte éthique, à l'instar de ce jugement du 19 septembre 2006 du tribunal de grande instance de Lyon qui a considéré que « si les demandeurs ont initialement évoqué et critiqué le dispositif d'alerte professionnelle mis en place, force est de constater que le texte remanié en ce qu'il le présente comme un moyen facultatif qui ne peut être utilisé que pour répondre à des intérêts dont la légitimité est établie (domaines comptables, contrôle des comptes et lutte contre la corruption), en ce que l'identité de l'émetteur est traitée de manière confidentielle et en ce que la personne visée bénéficie d'un droit d'accès aux renseignements et d'un droit de rectification, est conforme à la délibération de la Cnil du 8 décembre 2005 »[72]. En avril 2005 déjà, le juge des référés de Nanterre avait considéré que le document présenté au comité d'entreprise mettant en place une procédure d'alerte ne paraissait pas poser, au stade du référé et de l'évidence, de problème ni d'interprétation, ni de violation des droits du salarié, au motif qu'il s'agissait d'une procédure facultative sans sanctions ni conséquences d'aucune sorte[73].

Aux yeux de certains, ces précédents judiciaires dessinent de façon suffisamment précise le cadre applicable aux dispositifs d'alerte professionnelle. Les auteurs du rapport de mars 2007, pour leur part, notent qu'« à une époque où nombreux sont ceux qui aspirent légitimement à une plus grande sécurité juridique […], mieux vaut éviter une construction judiciaire par nature lente et conflictuelle d'un droit de l'alerte professionnelle ».

La légalisation des dispositifs d'alerte éthique professionnelle suscite encore indiscutablement débat.

---

[71] TGI Nanterre, 27 déc. 2006, Comité central d'entreprise Dupont de Nemours c/SAS Dupont de Nemours, n° 20006/02550.

[72] TGI Lyon, ch. urgences, 19 sept. 2006, Union départmentale CGT du Rhône, synd. CGT Bayer Cropscience c/Bayer Cropscience, v.
http://www.legalis.net/jurisprudence-decision.php3?id_article=1760.

[73] TGI Nanterre, ord. réf., 1er avr. 2005, CE ING Bank c/ING Bank France, inédit

CHAPITRE

34. Principes généraux pour le respect de la vie privée de l'employé

SECTION 0
ORIENTEUR

34.00

Plan du chapitre.

Sect. 1 Droits de l'employé

Sect. 2 Pertinence et finalité du traitement

Sect. 3 Mesures de protection

34.01

Textes applicables.

> Textes français.

Textes législatifs.

C. trav., art. L. 1121-1 et L. 1134-1 s.

Avis et recommandations.

Cnil, délib. n° 2002-001, 8 janv. 2002, concernant les traitements automatisés d'informations nominatives mis en œuvre sur les lieux de travail pour la gestion des contrôles d'accès aux locaux, des horaires et de la restauration — Cnil, délib. n° 2007-368, 11 déc. 2007, portant avis sur un projet de décret en Conseil d'État modifiant le décret n° 2005-1726 du 30 décembre 2005 relatif aux passeports électroniques.

34.02

Jurisprudence de référence.

> Sur le droit d'information de l'employé.

• **Soc. 6 avr. 2004,** n° 01-45.227, Sté Allied signal industrial Fibers c/M. Pacheco NPB, *Bull. civ.* V, n° 103 ; *Gaz. Pal.* 20 juill. 2004, n° 202, p. 31, note J. Bérenguer-Guillon et L. Maurel-Guignot — confirmation de **CA Nancy, ch. soc., 25 juin 2001,** M. Pacheco c/Sté Allied signal industrial Fibers, *Juris-Data* n° 145997 ; *Dr. ouvrier* 2002, n° 652.

Pour le jugement (infirmé) rendu en 1er ressort, v. **Cons. prud'h. Longwy, 3 déc. 1999.**

* V. s^s n° 34.10, égalt n° 14.24.

> Sur l'accès aux données de notation annuelle.

• **Soc. 23 oct. 2001,** n° 99-44.215, NPB, CANSSM c/Mme Vicheney, v. http://www.legifrance.gouv.fr/affichJuriJudi.do?oldAction=rechJuriJudi&idTexte=JURITEXT000007628680 — confirmation de **CA Paris, 18e ch., sect. A, 1er juin 1999.**

* V. s^s n° 34.12.

> Sur l'appréciation de la pertinence des données.

• **Civ. 1re, 29 mai 1984,** n° 82-12.232, CEMU c/Mme D… et a., *Bull. civ.* I, n° 176 — confirmation de **CA Rouen, 3e ch., 17 déc. 1981**.

* V. s^s n° 34.21.

34.03

> Rapport.

H. Bouchet (dir.), *La cybersurveillance sur les lieux de travail,* Cnil, mars 2004,, http://lesrapports.ladocumentationfrancaise.fr/BRP/044000175/0000.pdf.

> Article.

A. Saint-Martin, « La reconnaissance d'une présomption de professionnalité des messages électroniques du salarié », *RLDI* n° 34, janv. 2008, p. 29.

34.04

Questions principales.

• Quels sont les droits de l'employé sur les données à caractère personnel le concernant ?

* V. s^s n^os 34.10 s.

• Quelles sont les obligations à la charge de l'employeur ?

* V. s^s n^os 34.21 s.

SECTION 1
DROITS DE L'EMPLOYE

34.10
Droit d'information. V. s^s n^os 12.30 s. et 32.11 s.

34.11
Droits d'accès, de rectification et de suppression. Chaque employé, comme toute personne physique, dispose du droit de se faire communiquer toutes les informations le concernant dans un fichier et de faire rectifier ou supprimer les informations erronées. Il dispose également du droit de s'opposer à figurer dans un fichier, mais seulement pour des motifs légitimes qu'il appartient à l'employeur d'apprécier. Il ne peut pas s'opposer au recueil de données nécessaires au respect d'une obligation légale, par exemple pour des déclarations sociales obligatoires. En revanche, il peut s'opposer à ce que le comité d'entreprise soit destinataire des informations le concernant. Il doit cependant être clairement informé des conséquences qui en résultent pour lui (exclusion du bénéfice de tarifs réduits par exemple). Si les données ont déjà été transmises, le comité d'entreprise doit en être informé pour supprimer les données, conformément à la demande de l'employé concerné. Cette obligation pèse non seulement sur l'employeur mais également sur le comité d'entreprise ou tout autre organisme ayant, dans le secteur public, vocation à mettre en œuvre des fichiers informatiques de données personnelles des employés. Ces mentions doivent obligatoirement être portées sur le questionnaire visant à collecter des données personnelles concernant les employés. Dans les autres cas, la Commission nationale de l'informatique et des libertés (Cnil) considère que « l'affichage d'une note d'information dans les locaux ou la remise d'un document à l'employé peuvent constituer des mesures d'information adaptées »[74] (sur les droits des personnes concernées v. s^s n^os 12.41 s.).

34.12
Accès aux données de notation annuelle. À la suite de plusieurs plaintes déposées à l'encontre d'un employeur pour refus de communication à ses cadres de leur classement et de leur potentiel de carrière, la Cnil a considéré, lors de sa séance plénière du 8 mars 2007, que ce type de données est communicable au salarié concerné dès lors qu'elles ont été prises en compte pour décider de son augmentation de salaire, de sa promotion ou de son affectation. L'employé peut donc, conformément à l'article 39 de la loi du 6 janvier 1978 modifiée en août 2004, demander une copie du document comportant ces données.

Un arrêt de la Cour de cassation en date du 23 octobre 2001 avait déjà eu l'occasion de considérer que la non communication de sa fiche de notation à un salarié qui en fait la demande constitue un des éléments permettant de caractériser un comportement discriminatoire à son encontre[75].

SECTION 2
PERTINENCE ET FINALITE DU TRAITEMENT

34.21
Pertinence des données. Les données personnelles doivent être « adéquates, pertinentes et non excessives » au regard des objectifs poursuivis. La collecte des

---

[74] V. Cnil, *Guide pratique pour les employeurs,* p. 30.

[75] Soc. 23 oct. 2001, n° 99-44.215, NPB, CANSSM c/Mme Vicheney, v. http://www.legifrance.gouv.fr/affichJuriJudi.do?oldAction=rechJuriJudi&idTexte=JURITEXT000007628680.

informations concernant la santé ou les proches de l'employé serait contraire à ce principe. L'enregistrement du numéro de sécurité sociale est autorisé dans les fichiers de paie et de gestion du personnel pour permettre d'établir les bulletins de paie et les différentes déclarations sociales obligatoires (Décr. n° 91-1404, 27 déc. 1991 — CSS, art. R. 115-1 et R. 115-2) et pour la tenue des comptes d'épargne salariale (C. trav., art. L. 3341-6). Si la copie de l'avis d'imposition d'un employé peut être communiquée au comité d'entreprise pour permettre à celui-ci de calculer la contribution due par l'intéressé, il n'en est pas de même de la déclaration des revenus à raison du caractère privé des informations qui y figurent[76].

34.22

Usage légitime. Les données à caractère personnel doivent avoir un « usage déterminé et légitime ».

Ainsi, un dispositif de vidéosurveillance installé dans un lieu susceptible de porter atteinte à l'intimité de la vie privée des employés (douches par ex.) ou encore qui mettrait un employé ou un groupe de personnes sous une surveillance permanente serait illicite. Par ailleurs, la finalité annoncée doit être respectée.

Un lecteur de badge ne doit pas permettre de surveiller les allées et venues des employés ou encore d'accéder à des informations sur le détail de leurs consommations au sein du restaurant d'entreprise. La Cnil a émis un certain nombre de recommandations pour éviter de tels détournements de finalité dans sa délibération n° 02-001 du 8 janvier 2002[77].

34.23

Pas de commentaires excessifs dans les fichiers du personnel. La Cnil a condamné une société française, le 11 décembre 2007, à 40 000 euros d'amende en raison de commentaires subjectifs figurant dans le fichier de gestion des salariés[78]. Elle précise, dans sa délibération, que s'il est admis que des traitements de données à caractère personnel puissent comporter des zones commentaires destinées à enregistrer des informations de gestion telles que des résumés d'entretiens ou des indicateurs de suivi d'un dossier, ces mentions doivent être pertinentes, adéquates et non excessives au regard de la finalité du traitement. Le non-respect de cette obligation est susceptible d'entraîner l'application de l'article 226-18 du Code pénal. Dans le cas d'espèce, il s'agissait de personnes qui avaient été employées par l'entreprise qui n'avaient pas donné satisfaction.

SECTION 3
MESURES DE PROTECTION

34.31

Durée de conservation des données. Cette durée doit être précisée pour chaque fichier et en fonction de la finalité (par exemple, quelques jours à un mois maximum pour les enregistrements de vidéosurveillance). Elle exclut une conservation pour une durée indéterminée.

S'agissant des données de connexion (v. s^s n^os 27.00 s.), l'employeur doit donner le plus de précisions possibles sur la durée pendant laquelle les données de connexion permettant d'identifier le poste ou l'utilisateur s'étant connecté sont conservées ou sauvegardées. La Cnil préconise à ce titre la réalisation d'un bilan annuel : « les mesures de sécurité qui conduisent à conserver trace de l'activité

---

[76] Civ. 1re, 29 mai 1984, n° 82-12.232, *Bull. civ.* I, n° 176.

[77] Cnil, délib. n° 02-001, 8 janv. 2002, (norme simplifiée 42) concernant les traitements automatisés d'informations nominatives relatifs mis en œuvre sur les lieux de travail pour la gestion des contrôles d'accès aux locaux, des horaires et de la restauration, http://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000017653507

[78] Cnil, délib. n° 2007-368, 11 déc. 2007, portant avis sur un projet de décret en Conseil d'État modifiant le décret n° 2005-1726 du 30 décembre 2005 relatif aux passeports électroniques.

des utilisateurs ou de l'usage qu'ils font des technologies de l'information et de la communication ou qui reposent sur la mise en œuvre de traitements automatisés d'informations directement ou indirectement nominatives devraient faire l'objet d'un « bilan annuel informatique et libertés à l'occasion de la discussion du bilan social soumis au comité d'entreprise ou au comité technique paritaire ou à toute autre instance équivalente »[79].

34.32

Gestion des habilitations. L'employeur a l'obligation de définir une politique de sécurité pour garantir la confidentialité des données (L. 6 janv. 1978, art. 34). Certaines données ne peuvent être accessibles que pour certaines personnes, sauf la faculté de les transmettre à des tiers autorisés (inspection du travail, services fiscaux, *etc.*). De même, en présence d'un dispositif de vidéosurveillance, les images enregistrées ne peuvent être visionnées que par les seules personnes dûment habilitées à cet effet, dans le cadre de leurs attributions (pour plus de développements sur la vidéosurveillance v s[s] n[os] 30.00 s.).

[79] V. H. Bouchet (dir.), *La cybersurveillance sur les lieux de travail,* Cnil, mars 2004, p. 18, http://lesrapports.ladocumentationfrancaise.fr/BRP/044000175/0000.pdf.

CHAPITRE

35. Règles spécifiques aux administrateurs réseaux

SECTION 0
ORIENTEUR

35.00

Plan du chapitre.

Sect. 1 Principe : secret professionnel

Sect. 2 Exception : en présence d'un risque d'atteinte à la sécurité de l'entreprise

35.01

Textes applicables.

> Textes français. V. s^s n^o 3.01.

35.02

Jurisprudence de référence.

> Accès aux documents de l'employé .

• **Soc. 6 févr. 2001,** n^o 98-46.345, Sté Laboratoires pharmaceutiques Dentoria c/Mme Bardagiet et a., *Bull. civ.* V, n^o 43 ; *JCP G* 25 juill. 2001, n^o 30, p. 1514, note C. Puigelier ; *RTD civ.* oct.-déc. 2001, n^o 4, 880-882, note J. Mestre et B. Fages — cassation de **CA Toulouse, 4^e ch. soc., 23 oct. 1998.**

• **Soc. 18 mars 2003,** n^o 01-41.343, NPB, UMS c/Mme C…, *Gaz. Pal.* 25 sept. 2003, n^o 268, p. 37, note L. Maurel-Guignot — cassation de **CA St Denis de la Réunion, ch. soc., 28 nov. 2000**.

* V. s^s n^o 35.21, égalt n^os 31.24 et 33.22.

> Des mesures justifiées en cas d'atteinte à la sécurité.

• **CA Paris, 11^e ch., sect. A, 17 déc. 2001,** n^o 2000-07565, F. M…, H. H… et V. R… c/Min. Public et A. T…, *Gaz. Pal.* 8 mai 2002, p. 31, comm. S. Le Guillas.

* V. s^s n^o 35.21.

35.04

Questions principales.

• Quelles sont les obligations et responsabilités des administrateurs réseaux ?

* V. s^s n^o 35.12.

• Quelles sont les limites à leur pouvoir d'intervention ?

* V. s^s n^o 35.21.

SECTION 1
PRINCIPE : SECRET PROFESSIONNEL

35.11

Moyens de contrôle à distance. La question de la violation du secret des correspondances prend une dimension particulière avec les administrateurs réseaux dont la mission consiste à s'assurer du fonctionnement normal et de la sécurité des réseaux et systèmes au sein de l'entreprise. Leur fonction les conduit à avoir accès à des informations relatives aux utilisateurs (messagerie, données de connexion à internet, fichiers-logs, *etc.*). Ils ont généralement les moyens de contrôler à distance les postes de travail, par exemple pour assurer la télémaintenance des logiciels ou, plus généralement, pour prendre le contrôle du poste en lieu et place de l'utilisateur.

35.12

Respect des obligations de transparence et de proportionnalité. Les conditions d'intervention des administrateurs réseaux doivent être portées à la connaissance

des employés et des organes représentatifs du personnel au titre de l'obligation de transparence à la charge de l'employeur (sur ce principe v. s^{s} n^{os} 32.00 s.). Ces interventions doivent être strictement encadrées (information préalable de l'utilisateur et intervention avec son accord préalable, au besoin par *e-mails*) et limitées au bon fonctionnement des applications.

Le contrôle doit également être conforme au principe de proportionnalité (sur ce principe v. s^{s} n^{os} 32.00 s.) et respectueux du principe de finalité énoncés par la loi informatique et libertés.

La Commission nationale de l'informatique et des libertés (Cnil) a eu l'occasion de rappeler que toute utilisation de ces outils de la propre initiative des administrateurs réseaux ou sur ordre hiérarchique, par exemple à des fins de contrôle, « n'est ni conforme au principe de proportionnalité, ni respectueuse du principe de finalité posé par la loi informatique et libertés »[80].

35.13

Obligation de confidentialité renforcée. Les administrateurs réseaux sont tenus au secret professionnel et, plus généralement, à une obligation de discrétion professionnelle qui leur interdit de divulguer les informations qu'ils auraient été amenés à connaître dans l'exercice de leurs fonctions.

Cette règle est rappelée par la Cnil, dans son rapport consacré à la *Cybersurveillance sur les lieux de travail* (févr. 2004) que « les administrateurs de réseaux et systèmes, généralement tenus au secret professionnel ou à une obligation de discrétion professionnelle, ne doivent pas divulguer des informations qu'ils auraient été amenés à connaître dans le cadre de leurs fonctions, et en particulier lorsque celles-ci sont couvertes par le secret des correspondances ou relèvent de la vie privée des utilisateurs et ne mettent en cause ni le bon fonctionnement technique des applications, ni leur sécurité, ni l'intérêt de l'entreprise ». Elle précise de plus que les administrateurs ne sauraient être contraints de divulguer ces informations, « sauf disposition législative particulière en ce sens ».

Enfin, le Forum des droits sur l'internet indique pour sa part que « l'administrateur réseau devrait veiller à ne divulguer à personne au sein de l'entreprise, y compris à sa hiérarchie et à ses collègues, les informations personnelles qui concernent un salarié dont il peut avoir connaissance dans le cadre de ses fonctions ».

Aussi, des mesures de sécurité doivent être prises pour garantir la confidentialité des informations auxquelles les administrateurs réseaux ont accès dans l'exercice de leurs fonctions. Cette obligation de confidentialité devrait être rappelée dans le contrat de travail, voire même dans le règlement intérieur ou la charte d'utilisation des outils informatiques.

SECTION 2
EXCEPTION : EN PRESENCE D'UN RISQUE D'ATTEINTE A LA SECURITE DE L'ENTREPRISE

35.21

Mesures justifiées en cas d'atteinte à la sécurité. Ces règles connaissent cependant une limite, en cas de risque d'atteinte à la sécurité de l'entreprise ou de l'administration. C'est dans ce contexte que la cour d'appel de Paris a précisé, dans un arrêt du 17 décembre 2001, que « la préoccupation de la sécurité du réseau justifiait que les administrateurs de systèmes et de réseaux fassent usage de leurs positions et des possibilités techniques dont ils disposaient pour mener les investigations et prendre les mesures que cette sécurité imposait — de la même façon que la Poste doit réagir à un colis ou une lettre suspecte. Par contre, la divulgation du contenu des messages, et notamment du dernier qui concernait le conflit latent dont le laboratoire était le cadre, ne relevait pas de ces

[80] Cnil, *Guide pratique pour les employeurs,* p. 14.

objectifs »[81].

De même, l'employeur doit pouvoir accéder aux documents stockés dans l'ordinateur de son employé absent de son poste de travail (congés, maladie not.)[82]. La Cour de cassation, dans un arrêt du 18 mars 2003, a ainsi considéré que l'employé était tenu de communiquer son mot de passe ou les fichiers en sa possession lorsque le bon fonctionnement de son entreprise dépend des données détenues par cet employé[83].

[81] CA Paris, 11e ch., sect. A, 17 déc. 2001, F. M..., H. H... et V. R... c/Min. public et A. T..., *Gaz. Pal.* 8 mai 2002, p. 31, comm. S. Le Guillas ;
http://www.foruminternet.org/documents/jurisprudence/lire.phtml?id=240.

[82] Soc. 6 févr. 2001, no 98-46.345, NPB, *Bull. civ.* V, no 43 ; *JCP G* 2001, no 30, p. 1514, note C. Puigelier ; *RTD civ.* oct.-déc. 2001, no 4, 880-882, note J. Mestre et B. Fages ; *Gaz. Pal.* 20 mars 2001, no 79, p. 9.

[83] Soc. 18 mars 2003, no 01-41.343, NPB, *Gaz. Pal.* 25 sept. 2003, no 268, p. 37, note L. Maurel-Guignot.

CHAPITRE

36. Règles spécifiques aux opérations de recrutement

SECTION 0
ORIENTEUR

36.00

Plan du chapitre.

Sect. 1 Conditions de mise en œuvre

Sect. 2 Droits du candidat

Sect. 3 Mesures protectrices du candidat

36.01

Textes applicables.

> Textes français.

Texte législatif.

C. trav., art. L. 1221-6 et L 1221-8.

Avis et délibérations.

Cnil, délib. n° 02-017, 21 mars 2002, portant adoption de recommandation relative à la collecte et au traitement d'informations nominatives lors d'opérations de recrutement (abroge et remplace la Cnil, recomm. 85-44, 15 oct. 1985).

Cnil, Recomm. Pour mesurer la diversité des origines dans la lutte contre les discriminations du 5 juillet 2005

> Texte européen.

V. s^s n° 1.01 : Dir. n° 95-46, 24 oct. 1995, art. 10.

36.04

Questions principales.

• Quels sont les droits du candidat au recrutement ?

* V. s^s n^os 36.21 s.

• Quelles sont les garanties dont-il bénéficie ?

* V. s^s n^os 36.31 s.

SECTION 1
CONDITIONS DE MISE EN ŒUVRE

36.11

Formalités déclaratives. Les personnes chargées du recrutement doivent déclarer auprès de la Commission nationale de l'informatique et des libertés (Cnil) les traitements automatisés d'informations nominatives, préalablement à leur mise en œuvre (L. 6 janv. 1978, art. 22). Tout manquement à cette règle expose le responsable du traitement à des sanctions pénales (C. pén., art. 226-24).

36.12

Une finalité limitée au recrutement. Le Code du travail précise que « les informations demandées, sous quelque forme que ce soit, au candidat à un emploi ne peuvent avoir comme finalité que d'apprécier sa capacité à occuper l'emploi proposé ou ses aptitudes professionnelles. Ces informations doivent présenter un lien direct et nécessaire avec l'emploi proposé ou avec l'évaluation des aptitudes professionnelles. Le candidat est tenu de répondre de bonne foi à ces demandes d'informations » (C. trav., art. L. 1221-6).

La Cnil considère pour sa part que, sauf les cas particuliers justifiés par la nature d'un poste à pourvoir ou des règles en vigueur dans le pays étranger concerné par le poste, les questions suivantes sont contraires aux prescriptions légales : date d'entrée en France, date de naturalisation, modalités d'acquisition de la nationalité française, nationalité d'origine, numéros d'immatriculation ou d'affiliation aux régimes de sécurité sociale, détail de la situation militaire, adresse précédente, informations concernant l'entourage familial (conjoint notamment), état de santé (notamment taille, poids), statut de propriétaire ou de locataire, vie associative, domiciliation bancaire, emprunts souscrits.

Par ailleurs, pourrait constituer une collecte frauduleuse, déloyale ou interdite (L. 6 janv. 1978, art. 6), l'utilisation d'annonces pour constituer un fichier de candidatures ou encore la collecte d'informations auprès de l'environnement professionnel du candidat à l'insu de celui-ci.

Enfin, sont interdites la collecte et la conservation de données qui, directement ou indirectement, font apparaître les origines raciales ou les opinions politiques, philosophiques ou religieuses ou les appartenances syndicales, les informations relatives à la santé ou à la vie sexuelle des personnes (L. 6 janv. 1978, art. 6). La seule dérogation, sous réserve de l'accord exprès des intéressés, concerne la spécificité d'un poste à pourvoir.

SECTION 2
DROITS DU CANDIDAT

36.21

Droit d'information des candidats. Les candidats, comme toutes les personnes auprès desquelles sont recueillies des données à caractère personnel, disposent d'un droit d'information (i) du caractère obligatoire ou facultatif des réponses ; (ii) des conséquences à leur égard d'un défaut de réponse ; (iii) des personnes physiques ou morales destinataires des informations ; (iv) de l'existence d'un droit d'accès et de rectification (L. 6 janv. 1978, art. 32). Par ailleurs, ils ont le droit de s'opposer, pour des raisons légitimes, à ce que des informations nominatives les concernant fassent l'objet d'un traitement (L. 6 janv. 1978, art. 38).

Le candidat doit également être informé de l'identité du responsable du traitement et de la finalité du traitement auquel les données sont destinées (Dir. n° 95-46, 24 oct. 1995, art. 10). À ce titre, la Cnil émet deux recommandations :

(i) « (que) les personnes chargées du recrutement prennent toutes les dispositions nécessaires pour informer le candidat, dans un délai raisonnable, de l'issue donnée à sa candidature, de la durée de conservation des informations le concernant ainsi que de la possibilité de demander la restitution ou la destruction de ces informations ».

(ii) « (que) les personnes, dont les coordonnées sont enregistrées dans un fichier de candidats potentiels utilisé dans le cadre d'une activité par approche directe, soient informées des dispositions de l'article 27 de la loi du 6 janvier 1978, au plus tard lors du premier contact. Lorsque l'identité de l'employeur n'a pas été précisée lors de l'offre de poste, l'accord du candidat doit être recueilli préalablement à la transmission des informations nominatives à cet employeur. Dans le cas de collecte d'informations nominatives par le biais de connexions à distance, la Cnil recommande que le candidat à l'emploi soit informé de la forme, nominative ou non, sous laquelle les informations le concernant seront éventuellement diffusées en ligne ou transmises aux employeurs. Le candidat doit également être préalablement informé de toute éventuelle cession d'informations à d'autres organismes chargés de recrutement et être en mesure de s'y opposer ».

La Cnil rappelle également que « les informations collectées ne peuvent être utilisées que pour la proposition d'emploi à l'exclusion de toute autre finalité, notamment de prospection commerciale ».

Enfin, le candidat doit être expressément informé, « préalablement à leur mise en œuvre, des méthodes et techniques d'aide au recrutement utilisées à son égard » (C. trav., art. L. 1221-8 ; anc. L. 121-7). À ce titre, la Cnil recommande que « l'information concernant les méthodes d'aide au recrutement employées soit

dispensée préalablement par écrit sous une forme individuelle ou collective ».

36.22
Droit d'accès et de rectification. Un candidat peut exercer le droit d'accès et de rectification dont bénéficie chaque personne concernée sur les données le concernant, qu'il s'agisse des données collectées directement auprès de lui ou auprès de tiers ou encore des données issues des méthodes et techniques d'aide au recrutement. Il peut ainsi obtenir communication des informations le concernant et exiger leur rectification en cas d'inexactitude (L. 6 janv. 1978, art. 39). La Cnil recommande en conséquence que « tout candidat soit clairement informé des modalités d'exercice du droit d'accès et puisse obtenir sur sa demande toutes les informations le concernant, y compris les résultats des analyses et des tests ou évaluations professionnelles éventuellement pratiqués ». Elle recommande également que « la communication des informations contenues dans la fiche du candidat soit effectuée par écrit, la communication des résultats des tests ou évaluations devant être faite par tout moyen approprié au regard de la nature de l'outil utilisé ».

SECTION 3
MESURES PROTECTRICES DU CANDIDAT

36.31
Durée de conservation des données. Sauf autorisation de la Cnil, les données à caractère personnel ne doivent pas être conservées au delà de la durée indiquée dans la déclaration du traitement (L. 6 janv. 1978, art. 36). La Cnil recommande à ce titre que le candidat « soit informé de la durée pendant laquelle les informations le concernant seront conservées et du droit dont il dispose d'en demander, à tout moment, la suppression. En tout état de cause, la durée de conservation des informations ne devrait pas excéder deux ans après le dernier contact avec la personne concernée ». Cette mesure est préconisée pour tout candidat, que la procédure de recrutement ait abouti favorablement ou non.

36.32
Sécurité et confidentialité des données. Le responsable du traitement automatisé de données concernant les candidats à un recrutement doit s'engager à l'égard des candidats à prendre toutes mesures de sécurité et de confidentialité (L. 6 janv. 1978, art. 34). Les tiers à une procédure de recrutement ne peuvent donc pas avoir accès directement ou indirectement aux données.

36.33
Profils automatiques. Le candidat a le droit d'être informé des raisonnements utilisés dans les traitements automatisés d'aide à la sélection de candidatures (L. 6 janv. 1978, art. 22). Cependant, aucune décision de sélection de candidature impliquant une appréciation sur un comportement humain ne peut avoir pour seul fondement un traitement informatisé donnant une définition du profil ou de la personnalité du candidat (L. 6 janv. 1978, art. 10). Aussi, la Cnil recommande-t-elle de proscrire « les outils d'évaluation automatisés à distance excluant toute appréciation humaine ».

36.34
Outils statistiques de mesure des discriminations. La Cnil recommande de ne pas collecter des données relatives à l'origine raciale ou ethnique des employés ou candidats à un emploi et de ne pas procéder à l'analyse de la consonance du nom ou du prénom. En revanche, peuvent être recueillies et traitées des données telles que le nom du candidat à l'emploi ou de l'employé, son prénom, sa nationalité, sa nationalité d'origine, son lieu de naissance, la nationalité ou le lieu de naissance de ses parents, son adresse.

Par ailleurs, la Cnil considère qu'un rejet de candidature à une embauche ou à une promotion peut être le résultat de la prise en compte simultanée de plusieurs critères non discriminatoires, par exemple une expérience professionnelle. Le

facteur discriminant peut donc résulter de l'analyse statistique croisée de ces différents critères. Aussi, lorsque les questionnaires contiennent des données qui permettent l'identification indirecte de la personne interrogée, la Cnil recommande-t-elle que l'accès au contenu soit limité aux seules personnes spécialement chargées de l'étude, que « les résultats soient produits sous une forme statistique agrégée » de nature à garantir l'anonymat et que les questionnaires soient détruits une fois les réponses exploitées. Lorsque les questionnaires intègrent une donnée identifiante, la Cnil préconise le recours à des identifiants autres que ceux utilisés dans le cadre de la gestion des ressources humaines (tel que le numéro de sécurité sociale notamment), l'enregistrement des réponses dans un fichier distinct des fichiers de gestion des ressources humaines ainsi que la mise en œuvre d'une procédure d'anonymisation prévoyant l'effacement « non seulement de l'identité du candidat à un emploi, mais également de son adresse, de ses coordonnées téléphoniques et électroniques, de sa photographie, et de toute autre donnée permettant son identification ».

Sur ce point, il convient toutefois de signaler l'adoption par la Commission des lois de l'Assemblée nationale[84], d'un amendement au pojet de loi relatif à la maîtrise de l'immigration, à l'intégration et à l'asile. Cet amendement en date du 12 septembre 2007 s'inspire des observations et recommandations[85] de la Cnil en matière de mesures de la diversité. Elles visent à proposer de modifier la loi informatique et libertés afin de faciliter les recherches en matière de mesures de la diversité des origines, de la discrimination et de l'intégration, tout en améliorant la protection des données et le caractère scientifique des enquêtes. Le texte suggère notamment que les données faisant directement ou indirectement apparaître les origines raciales ou ethniques des personnes puissent être recueillies pour les besoins d'études ayant pour finalités « la mesure de la diversité des origines des personnes, de la discrimination et de l'intégration » mais que ces traitements soient soumis à l'autorisation de la Cnil et que les personnes concernées conservent leur droit d'opposition à ce traitement.

[84] Rapp. de la Commission des lois, http://www.assemblee-nationale.fr/13/rapports/r0160.asp.

[85] Cnil, recomm., 5 juill. 2005, pour mesurer la diversité des origines dans la lutte contre les discriminations, v. http://www.cnil.fr/index.php?id=1844.

CHAPITRE

37. Règles spécifiques aux organisations syndicales

SECTION 0

ORIENTEUR

37.00

Plan du chapitre.

Sect. 1 Conditions d'utilisation de l'internet et de l'intranet

Sect. 2 Règles protectrices de l'employé

37.01

Textes applicables.

> Textes français. V. s^{s} n^{o} 3.01 : C. trav., art. L. 2142-6 — L. n^{o} 82-689, 4 août 1982, relative aux libertés des travailleurs dans l'entreprise — L. n^{o} 2004-391, 4 mai 2004 relative à la formation professionnelle tout au long de la vie et au dialogue social, *JO* n^{o} 105, 5 mai, 7983 — L. n^{o} 2008-67, 21 janv. 2008, ratifiant l'ordonnance n^{o} 2007-329 du 12 mars 2007 relative au Code du travail (partie législative), *JO* n^{o} 0018, 22 janv., 1122.

37.02

Jurisprudence de référence.

> Liberté d'utilisation de la messagerie et de l'intranet sous condition d'un accord d'entreprise.

• **Soc. 25 janv. 2005,** n^{o} 02-30.946, Fédération des services CFDT et a. c/Sté Clear Channel France *Bull. civ.* V, n^{o} 19 ; *LPA* 8 mars 2005, n^{o} 47, p. 3, note A. Sauret et G. Picca — confirmation de **CA Paris, 14^{e} ch., sect. B, 31 mai 2002**.

• **Soc. 22 janv. 2008,** n^{o} 06-40.514, M. M. c/Crédit industriel et commercial, *RDT* 2008, p. 324 ; *Sem. soc. Lamy* n^{o} 1339, 2008 — confirmation de **CA Paris, 18^{e} ch., sect. D, 29 nov. 2005**.

• **Crim. 10 mai 2005,** n^{o} 04-84705, *Bull. crim.,* n^{o} 144.

* V. s^{s} n^{o} 37.11.

> Sur la liberté d'expression syndicale.

• **CAA de Nancy, 3^{e} ch., 2 août 2007,** cne de Lons le Saunier c/Elisabeth M…, *RLDI* 2007, n^{o} 31 — annulation de **TA Besançon, 1re ch., 19 déc. 2006,** Elisabeh M… c/Ville de Lons-Le-Saunier, RG n^{o} 0400718.

* V. s^{s} n^{o} 37.12.

• **Soc. 5 mars 2008,** n^{o} 06-18.907, sté TNS Secodip c/féd. CGT des stés d'études, *Gaz. Pal.* 26 avr. 2008, n^{o} 117, http://www.courdecassation.fr/jurisprudence_publications_documentation_2/actualite_jurisprudence_21/chambre_sociale_576/arrets_577/br_arret_11274.html — cassation de **CA Paris, 18^{e} ch. civ., 15 juin 2006,** Féd. CGT des stés d'études c/TNS Secodip, puis renvoi devant CA Paris.

Pour le jugement rendu (infirmé) en 1er ressort, v**. TGI Bobigny, 11 janv. 2005,** TNS Secodip c/Fédération CGT des Sociétés d'Etudes.

• **CA Paris, 18^{e} ch. C, 15 juin 2006,** Féd. CGT des stés d'études c/TNS Secodip, (préc.).

* V. s^{s} n^{o} 37.14.

37.04

Questions principales.

• Les syndicats peuvent-ils disposer d'un site internet dédié ?

* V. s^{s} n^{o} 37.11.

• Quelles sont les conditions de mise en œuvre d'un tel site ?

* V. s^{s} n^{os} 37.13 s.

• Quelles sont les garanties offertes aux employés dont les données personnelles sont exploitées par les syndicats ?

* V. s^{s} n^{os} 37.21 s.

SECTION 1

CONDITIONS D'UTILISATION DE L'INTERNET ET DE L'INTRANET

37.11

Un accord d'entreprise obligatoire. Il est prévu, dans le Code du travail, qu'un « accord d'entreprise peut autoriser la mise à disposition des publications et tracts de nature syndicale, soit sur un site syndical mis en place sur l'intranet de l'entreprise, soit par diffusion sur la messagerie électronique de l'entreprise. Dans ce dernier cas, cette diffusion doit être compatible avec les exigences de bon fonctionnement du réseau informatique de l'entreprise et ne doit pas entraver l'accomplissement du travail. L'accord d'entreprise définit les modalités de cette mise à disposition ou de ce mode de diffusion, en précisant notamment les conditions d'accès des organisations syndicales et les règles techniques visant à préserver la liberté de choix des salariés d'accepter ou de refuser un message» (C. trav., art. L.2142-6—L.n° 2004-391, 4 mai 2004—L.n° 2008-67, 21 janv. 2008).

Les organisations syndicales peuvent donc accéder à l'intranet, notamment pour constituer un blog syndical accessible à tous à l'intérieur de l'entreprise, et à la messagerie de l'entreprise à condition toutefois d'avoir préalablement négocié et conclu un accord d'entreprise.

À défaut d'accord d'entreprise, la jurisprudence se prononce pour l'interdiction de la diffusion — ce que confirme l'arrêt rendu le 25 janvier 2005[86] par la Cour de cassation. Dans cette affaire, le syndicat avait envoyé sur l'adresse électronique professionnelle de tous les employés un mail syndical. Il n'y avait ni accord d'entreprise, ni même autorisation de l'employeur.

Par ailleurs, en présence d'un accord d'entreprise, la Cour de casssation en fait une stricte application. Dans un arrêt du 22 janvier 2008, elle observe ainsi que l'accord d'entreprise subordonnait la faculté d'utilisation de la messagerie électronique pour la publication d'informations syndicales à l'existence d'un lien entre le contenu et la situation sociale existant dans l'entreprise, et que tel n'était pas le cas en l'espèce (Soc. 22 janv. 2008[87]).

On observe cependant que le texte ne concerne pas l'accès à ces moyens informatiques par les instances représentatives du personnel, notamment le comité d'entreprise ou encore les délégués du personnel.

37.12

Le droit syndical est une liberté fondamentale. Cette règle, énoncée par le tribunal administratif de Besançon, le 19 décembre 2006, précise que personne ne peut y apporter « des restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché »[88]. Il a considéré que le maire de la commune de Lons-Le-Saunier ne pouvait pas sanctionner d'un blâme l'une de ses employés, adjoint administratif des services de la ville et responsable syndical, qui avait fait un appel à manifestation en utilisant les messageries intranet et internet de la ville et a écarté l'argument du maire qui entendait se prévaloir du manquement de cette employée à ses obligations professionnelles en ne respectant pas l'interdiction d'utiliser la messagerie à des fins personnelles.

Mais procédant à une analyse différente du contenu du mail litigieux, la cour administrative d'appel de Nancy a estimé, dans sa décision du 2 août 2007[89], qu'il s'agissait d'un message de nature politique. Dans ces conditions, elle a estimé que le maire de Lons-le-Saunier avait légalement prononcé une sanction contre son employée syndicaliste dans la mesure où une note de service du 18 novembre 2003 interdisait au personnel l'usage de l'internet à des fins politiques.

---

[86] Soc. 25 janv. 2005, n° 02-30.946, *Bull. civ.* V, n° 19.

[87] Soc. 22 janv. 2008, n° 06-40.514, *Sem. soc. Lamy* n° 1339, 2008.

[88] TA Besançon, 1re ch., 19 déc. 2006, Elisabeh M… c/Ville de Lons-Le-Saunier, v. http://www.legalis.net/jurisprudence-decision.php3?id_article=1818.

[89] CAA Nancy, 3e ch., 2 août 2007, cne de Lons le Saunier c/Elisabeth M…, *RLDI* 2007, n° 31.

37.13
Respect du principe de finalité. La finalité du traitement doit être strictement respectée. Ainsi, si l'accord d'entreprise autorise la diffusion d'informations syndicales par voie électronique, les adresses de messagerie électronique des employés ne peuvent être utilisées que pour la diffusion de publications et de tracts de nature syndicale.

37.14
Respect des droits d'autrui. La question des limites posées à la liberté de communication syndicale à partir d'un site externe à l'entreprise a été tranchée par la chambre sociale de la Cour de cassation le 5 mars 2008[90].

Dans le cas d'espèce, un syndicat avait publié sur son site certaines informations confidentielles de l'entreprise : deux avis d'un cabinet d'expertise comptable sur les comptes de la société, plusieurs comptes-rendus des négociations contractuelles, des réunions du comité d'entreprise et des questions posées par les délégués du personnel. L'entreprise, considérant que cette diffusion lui portait préjudice, a saisi le tribunal de grande instance de Bobigny afin d'obtenir la suppression de ces rubriques.

Les juges de première instance ont fait droit à cette demande, considérant que quatre rubriques contenant des informations confidentielles n'avaient pas à être portées à la connaissance de tiers et de concurrents et que l'obligation de discrétion et de confidentialité de l'employé s'impose également aux « syndicats qui représentent les salariés au sein d'une entreprise » (TGI Bobigny, 11 janv. 2005[91]).

Cette analyse a été infirmée par la cour d'appel, dans son arrêt du 15 juin 2006 qui a retenu que « comme tout citoyen, un syndicat a toute latitude pour créer un site internet pour l'exercice de son droit d'expression directe et collective, qu'aucune restriction n'est apportée à l'exercice de ce droit, et qu'aucune obligation légale ou de confidentialité ne pèse sur les membres du syndicat, à l'instar de celle pesant en vertu de l'article L. 432-7, alinéa 2 du Code du travail sur les membres du comité d'entreprise ou représentants syndicaux, quand bien même il peut y avoir identité de personnes entre eux »[92].

Saisie sur pourvoi, la Cour de cassation a censuré à son tour la cour d'appel, car « si un syndicat a le droit de communiquer librement des informations au public sur un site Internet, cette liberté peut être limitée dans la mesure de ce qui est nécessaire pour éviter que la divulgation d'informations confidentielles porte atteinte aux droits des tiers ». La Haute juridiction s'est fondée sur l'article 10-2 de la Convention Européenne de Sauvegarde des Droits de l'Homme et des libertés fondamentales (CESDH) qui prévoit expressément que la liberté d'expression peut être soumise à certaines conditions et restrictions prévues par la loi, qui constituent des mesures nécessaires à la protection ou la réputation des droits d'autrui. Elle s'est également fondée sur la loi pour la confiance dans l'économie numérique qui prévoit que l'exercice de la liberté de communication par voie électronique peut être limité dans la mesure requise, notamment dans le cadre du respect de la liberté et de la propriété d'autrui.

Précédemment, la chambre criminelle de la Cour de cassation avait également sanctionné les propos publiés sur le site d'un syndicat, à raison de la mise en

---

[90] Soc. 5 mars 2008, n° 06-18.907, sté TNS Secodip c/féd. CGT des stés d'études : cass. arrêt CA Paris, 15 juin 2006 (renvoi devant la CA Paris), http://www.courdecassation.fr/jurisprudence_publications_documentation_2/actualite_jurisprudence_21/chambre_sociale_576/arrets_577/arret_no_11275.html ; http://www.legalis.net/jurisprudence-decision.php3?id_article=2227 ; *Gaz. Pal.* 26 avr. 2008, n° 117.

[91] TGI Bobigny, 11 janv. 2005, TNS Secodip c/Féd. CGT des stés d'études, *Gaz. Pal.* 20 juill. 2005, n° 101, p. 45-46 ; *Expertises* avr. 2005, p. 156 — pour une analyse critique de cette décision, v. G. Haas et O. de Tissot, « Des restrictions inacceptables à la liberté d'action des syndicats », *Expertises* avr. 2005, p. 145.

[92] CA Paris, 18e ch. C, 15 juin 2006, Féd. CGT des stés d'études c/TNS Secodip, http://www.courdecassation.fr/jurisprudence_publications_documentation_2/actualite_jurisprudence_21/chambre_sociale_576/arrets_577/br_arret_11274.html.

cause injurieuse d'un directeur de la société, dans des termes jugés comme excédant « la mesure admissible dans un tel cadre » (Crim. 10 mai 2005[93]).

SECTION 2
REGLES PROTECTRICES DE L'EMPLOYE

37.21
Droit d'opposition des employés. Les employés doivent pouvoir exercer leur droit d'opposition à l'envoi de tout message syndical sur leur messagerie professionnelle. À cet effet, ils doivent être informés préalablement de l'accord conclu et des modalités d'exercice de leur droit d'opposition. Ils doivent pouvoir exercer ce droit à tout moment et, à ce titre, ce droit doit leur être rappelé dans chaque message. Par ailleurs, la Cnil préconise de prévoir l'indication du caractère syndical du message de manière à favoriser la plus grande transparence quant à l'origine et à la nature du message.

37.22
Garantie de confidentialité. Les échanges électroniques entre les employés et les organisations syndicales sont confidentiels. À ce titre, la Cnil considère qu'« afin d'éviter toute possibilité d'utilisation détournée, l'employeur ne devrait pas pouvoir exercer de contrôle sur les listes de diffusion ainsi constituées. En effet, celles-ci sont susceptibles de révéler l'opinion favorable d'un salarié à l'égard d'une organisation, voire son appartenance à un syndicat déterminé, sur la base du choix opéré par ce salarié quant à son acceptation ou son refus de recevoir des messages à caractère syndical »[94].

[93] Crim. 10 mai 2005, n° 04-84.705, *Bull. crim.,* n° 144.
[94] Cnil, *Guide pratique pour les employeurs,* p. 28.

CHAPITRE

38. Règles et usages en vigueur à l'étranger

SECTION 0
ORIENTEUR

38.00

Plan du chapitre.

38.04

Question principale.

• Comment les instances internationales et les législations des autres pays appréhendent la question des technologies sur le lieu de travail ?

SECTION 1
SUR LE PLAN EUROPEEN

38.11

Cour européenne des droits de l'Homme. Le principe de protection de la vie privée de l'employé sur son lieu de travail a été affirmé à plusieurs reprises par la Cour européenne des droits de l'Homme [95] : « Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance » (Conv. EDH, art. 8). S'il n'est pas toujours appréhendé de la même manière, on retrouve dans l'ensemble l'esprit et la lettre de la Convention Européenne de Sauvegarde des Droits de l'Homme et des libertés fondamentales (CESDH). La préoccupation est toujours la même : la recherche d'un compromis entre le pouvoir de contrôle de l'employeur sur l'activité de ses employés et le respect de leur vie privée. Plusieurs textes formalisent, au plan européen et international, l'obligation d'information préalable de l'employé.

38.12

Recommandation n° R (89). La recommandation n° R (89) du Comité des ministres du Conseil de l'Europe aux États membres sur la protection des données à caractère personnel utilisées à des fins d'emploi, du 18 janvier 1989 précise, :

« 3. Information et consultation des employés :

3.1. Conformément aux législations et pratiques nationales et, le cas échéant, aux conventions collectives, les employeurs devraient informer ou consulter leurs employés ou les représentants de ceux-ci préalablement à l'introduction ou à la modification de systèmes automatisés pour la collecte et l'utilisation de données à caractère personnel concernant les employés. Ce principe s'applique également à l'introduction ou à la modification de procédés techniques destinés à contrôler les mouvements ou la productivité des employés.

3.2. L'accord des employés ou de leurs représentants devrait être recherché avant l'introduction ou la modification de tels systèmes ou procédés lorsque la procédure de consultation mentionnée au paragraphe 3.1. révèle une possibilité d'atteinte au respect de la vie privée et de la dignité humaine des employés, à moins que d'autres garanties appropriées ne soient prévues par la législation ou la pratique nationale. »

38.13

Recueil de directives pratiques sur la protection des données personnelles des travailleurs du Bureau international du travail en date du 7 octobre 1996. Ce

[95] Not. CEDH, 16 déc. 1992, aff. Niemietz c/Allemagne, req. n° 00013710/88, A-251 B § 29, *JDI* 1993, p. 755, obs. E. Decaux et P. Tavernier ; *D.* 1993, somm. 386, obs. J.-F. Renucci.

document prévoit notamment que : « les données personnelles collectées en relation avec la mise en œuvre de mesures techniques ou d'organisation visant à garantir la sécurité et le bon fonctionnement des systèmes d'information automatisés ne devraient pas servir à contrôler le comportement des employés » (point 5.4.).

Cependant, ce recueil prévoit qu'une surveillance électronique peut être mise en œuvre à certaines conditions : d'une part, les données recueillies à cette occasion ne doivent pas être l'unique source de l'évaluation de l'employé, d'autre part, dans les cas où une surveillance est mise en œuvre, les employés doivent avoir été informés à l'avance des motivations de cette surveillance, des périodes concernées, des techniques utilisées ainsi que des données collectées (point 6. du recueil). Il est ainsi indiqué qu'une surveillance permanente ne saurait être autorisée que pour des raisons de santé et de sécurité et en vue de protéger les biens de l'entreprise. Il est également indiqué que la surveillance ne saurait être secrète sauf si elle est autorisée par la législation nationale et s'il existe des « soupçons raisonnablement justifiés d'activités criminelles ou d'autres infractions graves », au titre desquels il convient d'inclure le harcèlement sexuel.

38.14
Avis du 29 mai 2002 du G 29. Il convient également de signaler l'avis émis le 29 mai 2002 par le G 29 (v. s^{s} n^{o} 15.18). Consacré à « la surveillance des communications électroniques » sur le lieu de travail[96], cet avis apparaît très largement inspiré des travaux et réflexions de la Commission nationale de l'informatique et des libertés (Cnil).

SECTION 2
PARTICULARITES NATIONALES

38.21
États-Unis. La question délicate de la cybersurveillance n'est pas appréhendée de la même manière aux États-Unis où l'employeur se voit souvent reconnaître le droit de prendre connaissance de la messagerie de ses employés. Les plus récents sondages[97] indiquent en effet que 46,5 % des entreprises examinent et stockent le contenu des courriels de leurs employés. En effet, si le secret de leurs correspondances est protégé par l'*Electronic Communications Privacy Act of 1986*[98] (18 USC §§ 2510 s.), l'employeur peut mettre sous surveillance le réseau de l'entreprise, ce qui, concrètement, lui donne le droit d'écouter en toute légalité les conversations téléphoniques de ses employés, ou de consulter leurs e-mails, encore que ces dérogations ne sont possibles que pour les besoins de l'entreprise et sous réserve que l'employé ait été préalablement prévenu de cette surveillance.

38.22
Angleterre. L'autorité chargée de la protection des données personnelles, l'Information Commissioner, a publié un code de la protection des données personnelles et des pratiques relatives à l'emploi[99]. Celui-ci encadre les conditions dans lesquelles l'employeur peut surveiller ses employés. Se fondant ainsi sur les dispositions du *Data Protection Act of 1998* (c. 29)[100] ce code « subordonne » la surveillance des salariés sur leur lieu de travail à deux principes : la transparence et la proportionnalité. Aussi, l'employeur doit-il non seulement prévenir ses employés des mesures de surveillance mises en place, mais il doit également éliminer toutes les informations personnelles « inutiles ou excessives », compte tenu de la relation de travail les liant.

---

[96] G 29, avis, 29 mai 2002,
http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2002/wp55_fr.pdf
[97] Sondage réalisé par l'ePolicy Institute : http://www.epolicyinstitute.com/survey/survey.pdf.
[98] http://cpsr.org/issues/privacy/ecpa86/.
[99] *The Employment Practices Data Protection Code,*
http://www.informationcommissioner.gov.uk/eventual.aspx?id=437.
[100] http://www.opsi.gov.uk/Acts/Acts1998/ukpga_19980029_en_1.